ΤΕΥΧΟΣ 42

Στο DVD new openSUSE 11.4

total ΧΑΚΕЯ

ΔΙΑΒΑΣΕ ΤΟ, ΑΝ ΜΠΟΡΕΙΣ!

ΜΕΓΑΛΟ ΑΦΙΕΡΩΜΑ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΜΙΑ ΤΡΑΝΤΑΧΤΗ ΑΠΟΔΕΙΞΗ ΓΙΑ ΤΟ ΟΤΙ Ο ΚΑΛΟΣ Ο ΧΑΚΕΡ ΔΕΝ ΚΟΛΛΑΕΙ ΣΤΟ ΛΕΙΤΟΥΡΓΙΚΟ

ΤΑ ΠΑΝΩ-ΚΑΤΩ: ΕΥΚΟΛΕΣ ΕΠΙΘΕΣΕΙΣ ΑΠΟ WINDOWS ΣΕ LINUX :S

ΤΕΡΜΑ ΤΟ ΑΓΧΟΣ: ΑΚΟΜΗ ΚΙ ΑΝ ΧΑΣΕΤΕ ΤΟ LAPTOP, ΔΕΝ ΘΑ ΒΡΟΥΝ ΤΙΠΟΤΑ Σ' ΑΥΤΟ!

ΛΑΒΕΤΕ ΜΕΤΡΑ ΩΣΤΕ ΚΑΝΕΙΣ ΚΑΙ ΠΟΤΕ ΝΑ ΜΗ ΔΙΑΒΑΣΕΙ ΤΟ MAIL ΣΑΣ!

ΟΙ ΝΟΜΟΙ ΤΟΥ ΧΑΚΕЯ

[illegible]

1. Ο [illegible]
2. Η [illegible]
3. Ο [illegible]
4. [illegible]
5. Π [illegible]
6. Κ [illegible]
7. Η [illegible]
8. Το [illegible]
9. Ε [illegible]
10. Η [illegible]

Οι Νόμοι του Χάκερ είναι μια δυναμική λίστα.
Στείλτε μας τις δικές σας ιδέες για νέους νόμους,
αλλαγές ή προσθήκες στο xaker@4pi.gr

total XAKER

ΤΕΥΧΟΣ 42

Μεγάλο αφιέρωμα στην κρυπτογραφία, γιατί η σωστή ασφάλεια πρέπει να αφορά *και* στα δεδομένα μας. Επίσης: Επιθέσεις από Windows σε Linux, γιατί ο καλός ο χάκερ *δεν* κολλάει στο λειτουργικό ;)

06 **Κρυπτογραφία δημοσίου κλειδιού ueber alles**

Ακούσατε τον administrator στο εργαστήριο ή στην εταιρεία σας να μιλά μ' ενθουσιασμό για προγράμματα sniffing και είστε κάπως ανήσυχοι; Ψάχνετε έναν τρόπο για να στέλνετε μηνύματα ή αρχεία χωρίς *κανένας* άσχετος στη διαδρομή να μπορεί να βλέπει τα περιεχόμενά τους; Αλήθεια, τι σας διαβεβαιώνει ότι τα mail που παίρνετε προέρχονται από εκείνους που υποτίθεται ότι τα στέλνουν;

28 **Χάστε το laptop σας, χωρίς άγχος**

Τι είναι το χειρότερο που μπορεί να σας συμβεί *μετά* το χάσιμο ή την κλοπή του laptop σας; Μα, το γεγονός ότι κάποιοι θ' αποκτήσουν πρόσβαση στα περιεχόμενα του δίσκου του. Φυσικά, το ίδιο ισχύει και για τα δεδομένα που βρίσκονται στο δίσκο ή στους δίσκους του PC σας.

42 **Επιθέσεις ναι, μόνο από το Linux όχι!**

Ό,τι και να πείτε, δίκιο θα 'χετε. Καλό το Linux, δεν διαφωνούμε, αλλά σας έχουμε πρήξει πια μ' αυτό! Χάθηκαν δηλαδή τ' άλλα λειτουργικά συστήματα που χρησιμοποιεί ο κοσμάκης; Όχι βέβαια, καθόλου δεν χάθηκαν. Αυτός ο «κοσμάκης» μάλιστα τα χρησιμοποιεί για οποιαδήποτε δουλειά μπορείτε να φανταστείτε. Ναι. Ακόμη και για penetration testing.

Χάκερ@4pi.gr

54

54 Διάβασέ το, αν μπορείς!

Δεν έχει καμία σημασία πώς θα φτάσει το mail ή τα αρχεία σας από το σημείο Α στο σημείο Β. Μπορεί να πάει απευθείας, μπορεί να περάσει πρώτα από το Γ, μπορεί και μέσω όλων των γραμμάτων του αλφάβητου. Σημασία έχει ότι κανείς δεν θα μπορέσει να τα υποκλέψει, όσο πονηρός ή/και ικανός κι αν είναι. Για την ακρίβεια –και για να μη λέμε ό,τι θέλουμε– δεν αποκλείεται να τα καταφέρει κι όντως να τα υποκλέψει. Ακόμα και τότε, όμως, θα του είναι εντελώς άχρηστα! Εκτός βέβαια κι αν *δεν* είχατε μεριμνήσει να χρησιμοποιήσετε το GnuPG.

total XAKEP

4π ΕΙΔΙΚΕΣ ΕΚΔΟΣΕΙΣ Α.Ε.

Εκδότης	Γιώργος Κοπελιάδης
Διευθυντής	Αντώνης Βαμβακάρης
Αρχισυντάκτης	Χρήστος Βαρελάς
Σύμβουλοι Σύνταξης	Σάββας Χατζησάββας
Σύνταξη	Π.Βαρελάς, Ν.Θωμάδης, Γ.Κουρκουτός, Χ.Λέκκος, Λ.Λημμάτη, Ν.Μουρατίδης, Π.Παπαπαύλου, Β.Σάμιος, Γ.Σαραντόπουλος,
Ανάπτυξη Λογισμικού	Κοσμάς Καρακατσάνης
Διεύθυνση Δημιουργικού	Πελαγία Γιακουμάκη
Διεύθυνση Σχεδιασμού	Ευριπίδης Δεσποτίδης
Καλλιτεχνική Επιμέλεια	Στέλιος Πουλάκος
Σχεδιασμός-Σελιδοποίηση	Σ. Κανσού, Α. Κατσά, Γ. Μαρτζούκος, Β. Ρουσιώτη
Διεύθυνση Παραγωγής	Μανόλης Καστρινάκης Μ. Μυλωνάς
Φωτογραφία	Γιάννης Γλυνός Ε. Κατσιγιαννάκη, Μ. Σαρρή
Διεύθυνση Διόρθωσης	Μαρία Αλεξίου Α.Βλαχοδήμου, Ε.Γλεζέλλη, Μ.Καστρινάκη, Ε.Παπανικολάου, Μ.Τικοπούλου
Εμπορική Διεύθυνση	Αδαμαντία Βλάχου
Διεύθυνση Μάρκετινγκ	Βασίλης Πάνου
Διεύθυνση Διαφήμισης	Μπέσσυ Μπουτεράκου
Συνδρομές-Παραγγελίες	Α.Μ. Γιοντζή, Α. Καϊτσιώτη, Ν. Μαρκαριάν
Λογιστήριο	Γ. Παυλίδης, Γ. Σπανόπουλος

4π ΕΙΔΙΚΕΣ ΕΚΔΟΣΕΙΣ Α.Ε.

Διευθύνων Σύμβουλος
Θόδωρος Σπίνουλας

Το total XAKER εκδίδεται από την 4π Ειδικές Εκδόσεις Α.Ε μετά από άδεια του Δημοσιογραφικού Οργανισμού Λαμπράκη Α.Ε. Η 4π Ειδικές Εκδόσεις Α.Ε. έχει την έδρα της Ηνιόχου 26 & Πάρ. Αττικής Οδού, 152 38, Χαλάνδρι, Γραφείο Σύνταξης: Ηνιόχου 26 & Πάρ. Αττικής Οδού, 52 38, Χαλάνδρι, τηλ.: 210 6070100, fax: 210 6070199, e-mail: xaker@4pi.gr. Εμπορικό Τμήμα: Ηνιόχου 26 & Πάρ. Αττικής Οδού, 152 38, Χαλάνδρι, τηλ.: 210 6070100, fax: 210 6070198, e-mail: ramad@4pi.gr. Κυκλοφορεί 11 φορές το χρόνο, στην αρχή κάθε μήνα. Για τους μήνες Αύγουστο-Σεπτέμβριο εκδίδεται ένα διπλό τεύχος. Εκτύπωση-βιβλιοδεσία: 3Ε Εκτυπωτική Α.Ε.

Όλες οι απόψεις που εκφράζονται στα ενυπόγραφα άρθρα δεν εκφράζουν απαραίτητα και τη γνώμη του περιοδικού. Χειρόγραφα, επιστολές ή διαφάνειες που αποστέλλονται προς δημοσίευση δεν επιστρέφονται, ανεξάρτητα από τη δημοσίευσή τους ή μη.
Το περιοδικό διατηρεί το δικαίωμα να περικόπτει τις επιστολές που δημοσιεύονται, με την προϋπόθεση ότι δεν μεταβάλλεται το νόημά τους. Απαγορεύεται η αναδημοσίευση οποιουδήποτε άρθρου ή μέρους άρθρου, σε οποιαδήποτε γλώσσα, χωρίς γραπτή άδεια.

total XAKER is published 11 times a year, by 4pi Special Publications S.A. under License by Lambrakis Press S.A. Editorial Director: Antony Vamvakaris. Editorial Office: 26, Iniohou str., 152 38, Halandri, Greece, tel.: +30210 6070100, fax: +30210 6070199, e-mail: xaker@4pi.gr.
Advertising-Sales: Bessy Bouterakou, tel.: +30210 6070082, fax: +30210 6070198, e-mail: ramad@4pi.gr.

Τα Επίσημα Ανεπίσημα στέκια μας

Είμαστε κοινωνικοί – ειδικά στον online κόσμο. Είμαστε αστείοι, ευφυείς και φινετσάτοι – ειδικά στον online κόσμο. Είναι βέβαιο ότι έχουμε καβαλήσει το καλάμι – και μάλλον το 'χουμε καβαλήσει στον online *και* στον offline κόσμο. Τώρα ετοιμάζουμε και το Parabing. Θα σας αρέσει.

GNOO-PEE-GEE, BABY ;)

Κρυπτογραφία δημοσίου κλειδιού über alles!

Ακούσατε τον administrator στο εργαστήριο ή στην εταιρεία σας να μιλά μ' ενθουσιασμό για προγράμματα sniffing και είστε κάπως ανήσυχοι; Ψάχνετε έναν τρόπο για να στέλνετε μηνύματα ή αρχεία χωρίς *κανένας* άσχετος να μπορεί να βλέπει τα περιεχόμενά τους στη διαδρομή; Αλήθεια, τι σας διαβεβαιώνει ότι τα mail που παίρνετε προέρχονται από εκείνους που υποτίθεται ότι τα στέλνουν; Φοβάστε μήπως τι θα βρουν στο laptop ή στο σκληρό δίσκο του υπολογιστή σας, σε περίπτωση που πέσει σε ξένα χέρια; Ας κάνουμε τώρα κι ένα διαφορετικό –αλλά σχετικό με τα προηγούμενα– ερώτημα: Τι θα λέγατε για μια εκπληκτικά αποτελεσματική μέθοδο προστασίας των ευαίσθητων δεδομένων σας από αδιάκριτα βλέμματα;

GnuPG

ΥΣΤΕΡΑ ΑΠΟ ΜΙΑ ΤΕΤΟΙΑ ΕΙΣΑΓΩΓΗ είν' αναμενόμενο να σκέφτεστε ότι αναφερόμαστε σε κάποια ισχυρή κι αποτελεσματική μέθοδο κρυπτογράφησης. Επιπρόσθετα, επειδή μας έχετε πλέον μάθει, ήδη υποψιάζεστε ότι αυτή η μέθοδος είναι δωρεάν, καθώς κι ότι τα σχετικά εργαλεία διατίθενται για κάθε λειτουργικό σύστημα. Πράγματι, έτσι έχουν τα πράγματα.
Αναλυτικότερα, στο παρόν κείμενο θα δούμε πώς εκμεταλλευόμαστε το σύστημα κρυπτογράφησης Ελεύθερου Λογισμικού GnuPG (GNU Privacy Guard), ώστε να διασφαλίζουμε το απόρρητο του mail μας ή/και να κρυπτογραφούμε όποια αρχεία θέλουμε. Έτσι, ακόμα κι όταν το mail αποστέλλεται μέσω κάποιου server που δεν υποστηρίζει ασφαλείς, κρυπτογραφημένες συνδέσεις, το μόνο που θα μπορέσουν να δουν οι περίεργοι από τα μηνύματα που έχουμε επιλέξει να κρυπτογραφήσουμε θα 'ναι κάτι εντυπωσιακοί σωροί από απόλυτες ασυναρτησίες. Τα ίδια θα πάθουν και με τα αρχεία που επίσης έχουμε επιλέξει να κρυπτογραφήσουμε – ακόμα κι αν έχουν πάρει στην κατοχή τους ολόκληρο τον υπολογιστή μας. Σημειώστε, μάλιστα, ότι στην πράξη δεν θα 'χουν καμία ελπίδα για αποκρυπτογράφηση, εκτός βέβαια κι αν αποκτήσουν πρόσβαση στο ιδιωτικό μας κλειδί. Αλλά ας μην προτρέχουμε.
Θα ξεκινήσουμε την εκτενή κάλυψή μας στο GnuPG με μια προαιρετική εισαγωγή στις έννοιες της κρυπτογραφίας δημοσίου κλειδιού. Αμέσως μετά θα προχωρήσουμε στη διαχείριση του όλου συστήματος που υλοποιεί το GnuPG. Λίγο παρακάτω, στο άρθρο που αρχίζει από τη σελίδα 54 του τεύχους που κρατάτε στα χέρια σας, περνάμε και σε μια σειρά από πρακτικά παραδείγματα χρήσης, ενώ βλέπουμε κι ορισμένα προγράμματα που διευκολύνουν σημαντικά τη σχέση μας με το GnuPG :D
Για τη συνέχεια πάντως υποθέτουμε ότι έχετε κάποιες βασικές γνώσεις περί κρυπτογραφίας δημοσίου κλειδιού (public key encryption). Αν όχι, μην ανησυχείτε: Μπορείτε είτε να κάνετε μια παράκαμψη και να μελετήσετε το σχετικό λήμμα της Wikipedia (http://en.wikipedia.org/wiki/Public_key_cryptography) είτε να διαβάσετε την ενότητα που ακολουθεί, στην οποία ουσιαστικά κάνουμε μια σύντομη αλλά περιεκτική εισαγωγή στην κρυπτογραφία δημοσίου κλειδιού.

WHAT THE HECK IS THAT GNOO-PEE-GEE ANYWAYS?

Το GnuPG –στο εξής GPG– είν' ένα δημοφιλές σύστημα κρυπτογράφησης δημοσίου κλειδιού το οποίο, μεταξύ άλλων, διασφαλίζει ότι κανείς άλλος πλην των θεμιτών παραληπτών δεν θα διαβάζει το mail ή θα βλέπει τα αρχεία που αποστέλλουμε. Παρέχει επίσης κι έναν μηχανισμό πιστοποίησης (authentication), ούτως ώστε να 'μαστε βέβαιοι για την πραγματική ταυτότητα των αποστολέων.
Η όλη ιδέα βασίζεται σ' ένα μηχανισμό δύο κλειδιών (keypair): το δημόσιο (public) και το ιδιωτικό (private) ή αλλιώς μυστικό (secret) κλειδί. Κάθε τέτοιο ζεύγος είναι μοναδικό, δηλαδή σε κάθε ιδιωτικό κλειδί αντιστοιχεί ένα μόνο δημόσιο κι αντίστροφα. Τώρα, ένα μήνυμα ή αρχείο που έχει κρυπτογραφηθεί με χρήση

του ιδιωτικού κλειδιού μπορεί ν' αποκρυπτογραφηθεί *μόνο* από το αντίστοιχο δημόσιο. Αντίστροφα, ένα μήνυμα ή αρχείο που έχει κρυπτογραφηθεί με χρήση του δημοσίου κλειδιού, μπορεί ν' αποκρυπτογραφηθεί *μόνο* από το αντίστοιχο ιδιωτικό. Όπως φανερώνουν και τα ονόματά τους, το δημόσιο κλειδί διανέμεται ελεύθερα, ενώ το ιδιωτικό διατηρείται από τον κάτοχό του ως (επτασφράγιστο) μυστικό.

Δείτε τώρα τι σημαίνουν τα προηγούμενα στην πράξη. Το δημόσιο κλειδί που διαθέτουμε, επιτρέπει σ' άλλους να κρυπτογραφούν mail ή αρχεία που προορίζουν για μας. Είναι βέβαιοι ότι μόνο εμείς θα μπορούμε να τα διαβάζουμε, αφού εμείς και μόνο εμείς είμαστε οι κάτοχοι του αντίστοιχου ιδιωτικού κλειδιού παρουσία του οποίου είναι δυνατή η αποκρυπτογράφηση.

Το δε ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση mail ή αρχείων που στέλνουν σ' εμάς κι έχουν κρυπτογραφηθεί με χρήση του αντίστοιχου δημοσίου κλειδιού. Με το ιδιωτικό μας κλειδί μπορούμε επίσης να υπογράφουμε (sign) mail ή αρχεία που στέλνουμε ή/και δημοσιεύουμε, ώστε κάθε ενδιαφερόμενος να παίρνει το δημόσιο κλειδί μας, να ελέγχει αν μπορεί ν' αποκρυπτογραφήσει την υπογραφή κι έτσι να επαληθεύει, αν πραγματικά είμαστε εμείς οι αποστολείς/κάτοχοι κι όχι κάποιος άλλος που υποδύεται εμάς. Και φυσικά, όποτε στέλνουμε ένα μήνυμα ή αρχείο έχουμε τη δυνατότητα να το κρυπτογραφούμε και ταυτόχρονα να το υπογράφουμε κιόλας.

Όπως είπαμε λίγο πριν, κάθε ζεύγος ιδιωτικού-δημοσίου κλειδιού είναι μοναδικό. Συνεπώς, όταν αποστέλλουμε ένα κρυπτογραφημένο μήνυμα ή αρχείο σε παραπάνω από έναν παραλήπτες, θα πρέπει να διαθέτουμε τα δημόσια κλειδιά όλων. Τα δημόσια κλειδιά των παραληπτών που μας ενδιαφέρουν φυλάσσονται στο λεγόμενο δακτύλιο κλειδιών (keyring), ούτως ώστε να μπορούμε εύκολα να κρυπτογραφούμε μηνύματα/αρχεία που απευθύνονται σε πολλαπλούς αποδέκτες. Το δικό μας δημόσιο κλειδί συστήνεται να το αποθηκεύουμε σε κάποιον από τους δημόσιους διακομιστές δημοσίων κλειδιών (public keyservers), έτσι ώστε άλλοι χρήστες να μπορούν να το παίρνουν εύκολα και να μας στέλνουν κρυπτογραφημένη αλληλογραφία ή/και αρχεία.

Επιτρέπεται να διαθέτουμε παραπάνω από ένα ζεύγη κλειδιών, π.χ., ένα για την προσωπική κι ένα για την επαγγελματική μας αλληλογραφία. Σε κάθε περίπτωση, το ιδιωτικό κλειδί θα πρέπει να προστατεύεται από μια συνθηματική φράση (passphrase), ώστε ακόμη κι αν πέσει στα χέρια τρίτων αυτοί να μην μπορούν να το χρησιμοποιήσουν χωρίς να γνωρίζουν το passphrase. Πάντως ασχέτως αν έχουμε ένα ή περισσότερα ζεύγη κλειδιών, οφείλουμε να προστατεύουμε ως κόρη οφθαλμού το ιδιωτικό ή τα ιδιωτικά. Βλέπετε, αν κάποιος αποκτήσει πρόσβαση σε ιδιωτικό μας κλειδί και γνωρίζει και την αντίστοιχη συνθηματική φράση, όχι μόνο θα μπορεί να διαβάζει την κρυπτογραφημένη μας αλληλογραφία αλλά, ακόμα χειρότερα, θα μπορεί να υποδύεται εμάς. Στην περίπτωση που συμβεί κάτι τέτοιο –και φυσικά υποπέσει στην αντίληψή μας– το GPG παρέχει ένα μηχανισμό ανάκλησης, με βάση τον οποίο μπορούμε να ακυρώσουμε την ισχύ του δημοσίου κλειδιού μας, επομένως κι ολόκληρου του keypair.

ΠΟΥ ΘΑ ΤΟ ΒΡΩ; ΘΑ ΔΥΣΚΟΛΕΥΤΩ, ΓΕΝΙΚΩΣ;

Το κατεξοχήν σύστημα κρυπτογράφησης δημοσίου κλειδιού είναι το GnuPG (GNU Privacy Guard) ή απλά GPG (www.gnupg.org). Αποτελεί Ελεύθερο Λογισμικό, συμμορφώνεται με το πρότυπο του OpenPGP (www.openpgp.org/about_openpgp) και, όπως ήδη σας προϊδεάσαμε στην εισαγωγή, πρακτικά διατίθεται *δωρεάν* για κάθε λειτουργικό σύστημα. Οι χρήστες του Linux δεν χρειάζεται καν να το κατεβάσουν από κάπου, αφού κατά 99,37652% εγκαθίσταται με τη διανομή τους. Όσον αφορά στην οικογένεια του BSD, το GPG υπάρχει στα αντίστοιχα ports tree και η εγκατάστασή του είναι πανεύκολη. Πέρα από τον κόσμο του Unix, μια εκδοχή του GPG για Windows διατίθεται από το

`www.gpg4win.org`

ενώ μια για Mac OS X από το

`http://macgpg.sourceforge.net`

Στη συνέχεια θα δουλέψουμε σε περιβάλλον openSUSE. Έχετε, ωστόσο, υπόψη ότι όσα δούμε εφαρμόζονται εντελώς παρόμοια σε κάθε άλλη διανομή Linux, εκδοχή του BSD ή οποιοδήποτε άλλο λειτουργικό σύστημα.

Όσον αφορά τώρα στο ζήτημα της δυσκολίας, όλα εξαρτώνται από το πού βρίσκεστε αυτή τη στιγμή. Αν, π.χ., γνωρίζετε τι θα πει συμμετρική κι ασύμμετρη κρυπτογραφία (ή αλλιώς κρυπτογραφία δημοσίου κλειδιού), καθώς και τι είναι οι ψηφιακές υπογραφές, τότε όλα θα 'χουν νόημα ευθύς εξαρχής. Αν πάλι δεν έχετε ασχοληθεί με τέτοια ζητήματα όμως διαβάσατε ήδη την ενότητα «What the heck is gnoo-pee-gee anyways?» και τώρα στο άκουσμα και μόνο της λέξης «κρυπτογρφία» η φαντασία σας εξάπτεται, τότε σίγουρα θα γοητευτείτε από την απλότητα και τη δύναμη της κρυπτογραφίας δημοσίου κλειδιού. Αυτό και μόνο είν' αρκετό για ν' απλοποιήσει διαδικασίες που σ' άλλες περιπτώσεις θα φάνταζαν στρυφνές, περίπλοκες ή ακόμη και δυσνόητες. Αλλά ας αφήσουμε τα πολλά λόγια – ώρα για δράση!

ΔΗΜΙΟΥΡΓΙΑ ΖΕΥΓΟΥΣ ΚΛΕΙΔΙΩΝ

Είναι η πρώτη μας δουλειά, εκτός βέβαια κι αν έχουμε ήδη φτιάξει το keypair μας. Σ' ένα παράθυρο τερματικού, λοιπόν, πληκτρολογούμε τα ακόλουθα (τονισμένο με κίτρινο χρώμα είναι το input του χρήστη):

```
sub0@opensuse:~> gpg --gen-key
gpg (GnuPG) 2.0.16; Copyright (C) 2009 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

```
gpg: directory `/home/sub0/.gnupg' created
gpg: new configuration file `/home/sub0/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/sub0/.gnupg/gpg.conf' are not yet
active during this run
gpg: keyring `/home/sub0/.gnupg/secring.gpg' created
gpg: keyring `/home/sub0/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: subZraw
Email address: subZraw@parabing.com
Comment: This ain't Jim Beam
You selected this USER-ID:
    "subZraw (This ain't Jim Beam) <subZraw@parabing.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

gpg: problem with the agent: Bad CA certificate

We need to generate a lot of random bytes. It is a good idea to
perform
some other action (type on the keyboard, move the mouse, utilize
the
```

```
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/sub0/.gnupg/trustdb.gpg: trustdb created
gpg: key EBDCE7DA marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f,
1u
pub   2048R/EBDCE7DA 2011-03-12
      Key fingerprint = A34A B306 90A3 A042 61F6  163F 2B57 FA04
EBDC E7DA
uid                  subZraw (This ain't Jim Beam) <subZraw@para
bing.com>
sub   2048R/6A85AB25 2011-03-12
sub0@opensuse:~>
```

Και ναι, μόλις δημιουργήσαμε επιτυχώς ένα keypair για το χρήστη με πλήρες όνομα subZraw και διεύθυνση αλληλογραφίας subZraw@parabing.com. Επειδή μάλιστα σκοπεύουμε να διανείμουμε το δημόσιο κλειδί, βάλαμε ένα υπαρκτό e-mail address. Όσον αφορά στους τύπους και στο μήκος των κλειδιών, αφήσαμε τις προεπιλογές (αμφότερα τύπου RSA, μήκους 2048 bits έκαστο). Εξάλλου, μια και δεν είμαστε εντελώς τρελαμένοι με το θέμα της ασφάλειας, δεν ορίσαμε ημερομηνία λήξης για το δημόσιο κλειδί (key does not expire). Κάτι που *δεν* φαίνεται παραπάνω είναι η προτροπή του GNOME keyring daemon για τον ορισμό μιας συνθηματικής φράσης (passphrase) που θα προστεύει το ιδιωτικό κλειδί.
Το passphrase είναι κάτι σαν password αλλά έχει τη δυνατότητα να 'ναι περισσότερο πολύπλοκο, αφού επιτρέπεται να περιλαμβάνει κενά. Κάθε φορά που για οποιονδήποτε λόγο πρόκειται να χρησιμοποιηθεί το ιδιωτικό κλειδί θα απαιτείται η πληκτρολόγηση του passphrase. Αυτή είναι μια πολύ καλή δικλείδα ασφαλείας, αφού ακόμα και να πάρει κάποιος το ιδιωτικό μας κλειδί δεν θα μπορεί να το χρησιμοποιήσει αν *δεν* γνωρίζει και το αντίστοιχο passphrase.
Τελικά, το εργαλείο gpg έφτιαξε ένα νέο κατάλογο με όνομα .gnupg μέσα στο γονικό του χρήστη μας (sub0) κι εκεί αποθήκευσε το νέο ζεύγος κλειδιών. Μέσα στον ίδιο κατάλογο μπορούμε να δημιουργήσουμε κι άλλα keypairs, π.χ., για διαφορετικούς λογαριασμούς e-mail. Επίσης, στον ~/.gnupg βρίσκεται και το keyring με τα δημόσια κλειδιά του δικού μας αλλά κι άλλων χρηστών. Προς το παρόν βέβαια το keyring αυτό έχει ένα μόνο δημόσιο κλειδί: το δικό μας. Προκειμένου να δούμε πληροφορίες που το αφορούν, γράφουμε

```
sub0@opensuse:~> gpg --list-keys
/home/sub0/.gnupg/pubring.gpg
```

```
----------------------------
pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (This ain't Jim Beam) <subZraw@para-
bing.com>
sub   2048R/6A85AB25 2011-03-12
sub0@opensuse:~>
```

Αν τώρα θέλουμε να χρησιμοποιούμε το δημόσιο κλειδί μας για περισσότερες από μία διευθύνσεις e-mail, τότε αρκεί να τις προσθέσουμε από το interactive environment του gpg ως ακολούθως.

```
sub0@opensuse:~> gpg --edit-key EBDCE7DA
gpg (GnuPG) 2.0.16; Copyright (C) 2009 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

pub  2048R/EBDCE7DA  created: 2011-03-12  expires: never       us-
age: SC
                     trust: ultimate      validity: ultimate
sub  2048R/6A85AB25  created: 2011-03-12  expires: never       us-
age: E
[ultimate] (1). subZraw (This ain't Jim Beam) <subZraw@parabing.
com>

gpg> adduid
Real name: subZraw
Email address: subZraw@defiant.gr
Comment: Underworld SA
You selected this USER-ID:
    "subZraw (Underworld SA) <subZraw@defiant.gr>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

You need a passphrase to unlock the secret key for
user: "subZraw (This ain't Jim Beam) <subZraw@parabing.com>"
2048-bit RSA key, ID EBDCE7DA, created 2011-03-12

pub  2048R/EBDCE7DA  created: 2011-03-12  expires: never       us-
age: SC
                     trust: ultimate      validity: ultimate
```

```
sub  2048R/6A85AB25  created: 2011-03-12  expires: never      us-
age: E
[ultimate] (1)  subZraw (This ain't Jim Beam) <subZraw@parabing.
com>
[ unknown] (2). subZraw (Underworld SA) <subZraw@defiant.gr>

gpg> quit
Save changes? (y/N) y
sub0@opensuse:~>
```

Στην εντολή gpg --edit-key δώσαμε το ID του δημοσίου κλειδιού μας, το οποίο είδαμε προηγουμένως στην πρώτη γραμμή των αποτελεσμάτων της εντολής gpg --list-keys. Φυσικά, για να προχωρήσουν οι αλλαγές μάς ζητήθηκε και το passphrase του ιδιωτικού μας κλειδιού. Το interactive environment του gpg το εγκαταλείψαμε πληκτρολογώντας quit και μετά πατώντας το πλήκτρο [Y], ώστε να επικυρώσουμε τις αλλαγές.

ΔΗΜΙΟΥΡΓΙΑ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΑΝΑΚΛΗΣΗΣ

Ένα πιστοποιητικό ανάκλησης θα φανεί ιδιαίτερα χρήσιμο στην περίπτωση που το ιδιωτικό μας κλειδί πέσει σε ξένα χέρια. Για να το δημιουργήσουμε, ας θυμηθούμε το ID του δημοσίου κλειδιού:

```
sub0@opensuse:~> gpg --list-keys
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f,
1u
/home/sub0/.gnupg/pubring.gpg
-----------------------------
pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
uid                  subZraw (This ain't Jim Beam) <subZraw@para
bing.com>
sub   2048R/6A85AB25 2011-03-12
sub0@opensuse:~>
```

Το ID του δικού μας είναι EBDCE7DA, οπότε γράφουμε:

```
sub0@opensuse:~> gpg --output revoke.asc --gen-revoke EBDCE7DA

sec  2048R/EBDCE7DA 2011-03-12 subZraw (Underworld SA) <subZraw@
defiant.gr>
```

```
Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 0
Enter an optional description; end it with an empty line:
> I need to revoke this one, for reasons I'd really like to forget
:S
>
Reason for revocation: No reason specified
I need to revoke this one, for reasons I'd really like to forget
:S
Is this okay? (y/N) y

You need a passphrase to unlock the secret key for
user: "subZraw (Underworld SA) <subZraw@defiant.gr>"
2048-bit RSA key, ID EBDCE7DA, created 2011-03-12

ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory
gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in
case
your media become unreadable.  But have some caution:  The print
system of
your machine might store the data and make it available to others!
sub0@opensuse:~>
```

Παρατηρήστε ότι πληκτρολογήσαμε μια σύντομη εξήγηση για το λόγο της ανάκλησης. Προκειμένου να δημιουργηθεί το ίδιο το πιστοποιητικό ανάκλησης (αρχείο revoke.asc) χρειάστηκε να πληκτρολογήσουμε το passphrase του αντίστοιχου ιδιωτικού κλειδιού. Μετά τη δημιουργία του πιστοποιητικού οφείλουμε να το αντιγράψουμε, μαζί μ' ολόκληρο τον κατάλογο ~/.gnupg, σ' ένα CD ή thumb drive, το οποίο και θα φυλάξουμε σ' ένα ασφαλές μέρος.

ΔΗΜΟΣΙΕΥΣΗ ΚΑΙ ΕΙΣΑΓΩΓΗ ΣΕ/ΑΠΟ KEYSERVER

Αν θέλετε να επικοινωνείτε κρυπτογραφημένα μόνο με συγκεκριμένους χρήστες, τότε είναι εύκολο ν' ανταλλάξετε δημόσια κλειδιά, π.χ., μέσω απλού e-mail. Το ίδιο ισχύει αν θέλετε ν' ανταλλάσετε κρυπτογραφημένα αρχεία *πάλι* με συγκεκριμένους χρήστες (βλ. σχετικές ενότητες παρακάτω). Από την άλλη, στην περίπτωση που επιθυμείτε να 'χει πρόσβαση στο δημόσιο κλειδί σας οποιοσδήποτε ενδιαφερόμενος, τότε οφείλετε να το ανεβάσετε σ' έναν public keyserver. Υπάρχουν διάφοροι keyservers και πολλοί εξ αυτών ανταλάσσουν κλειδιά μεταξύ τους. Εκείνος που ορίζεται μέσα στο αρχείο ρυθμίσεων ~/.gnupg/gpg.conf είναι μια χαρά (αν θέλετε ανοίξτε το αρχείο μ' έναν text editor και ψάξτε για την οδηγία keyserver). Ας δούμε ένα παράδειγμα με το δημόσιο κλειδί του subZraw. Κατ' αρχάς, πριν το ανεβάσουμε στον public keyserver πρέπει να θυμηθούμε το ID του:

```
sub0@opensuse:~> gpg --list-keys
/home/sub0/.gnupg/pubring.gpg
-----------------------------
pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
uid                  subZraw (This ain't Jim Beam) <subZraw@para
bing.com>
sub   2048R/6A85AB25 2011-03-12
sub0@opensuse:~>
```

Καλώς. Η δημοσίευση γίνεται απλά πληκτρολογώντας

```
sub0@opensuse:~> gpg --send-keys EBDCE7DA
gpg: sending key EBDCE7DA to hkp server keys.gnupg.net
sub0@opensuse:~>
```

Τέλεια. Ας υποθέσουμε τώρα ότι θέλουμε να εισαγάγουμε στο public keyring μας το public key κάποιου άλλου χρήστη, ας πούμε του Richard Stallman, του πατέρα του Ελεύθερου Λογισμικού. Μια διεύθυνση αλληλογραφίας που χρησιμοποιεί δημοσίως είναι η rms@gnu.org και είναι πολύ πιθανό γι' αυτή να χρησιμοποιεί κάποιο δημόσιο κλειδί. Αλλά δεν χρειάζεται να μένουμε στις υποθέσεις:

```
sub0@opensuse:~> gpg --search-keys rms@gnu.org
gpg: searching for "rms@gnu.org" from hkp server keys.gnupg.net
(1)     Richard Stallman (Chief GNUisance) <rms@gnu.org>
          1024 bit DSA key 135EA668, created: 2001-03-05
(2)     Richard M. Stallman (Chief GNUisance) <rms@gnu.org>
          1024 bit DSA key A839EC1A, created: 2000-12-30
Keys 1-2 of 2 for "rms@gnu.org".  Enter number(s), N)ext, or Q)uit
> 1
```

```
gpg: requesting key 135EA668 from hkp server keys.gnupg.net
gpg: key 135EA668: public key "Richard Stallman (Chief GNUisance)
<rms@gnu.org>" imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f,
1u
gpg: Total number processed: 1
gpg:               imported: 1
sub0@opensuse:~>
```

Πολύ ωραία. Βλέπουμε ότι ο Stallman έχει δύο δημόσια κλειδιά. Αν και θα μπορούσαμε να εισαγάγουμε και τα δύο, επιλέγουμε μόνο το νεότερο. Εύκολα θα επαληθεύσουμε, αν η εισαγωγή του δημοσίου κλειδιού του Stallman στο public keyring μας πραγματοποιήθηκε επιτυχώς:

```
sub0@opensuse:~> gpg --list-keys
/home/sub0/.gnupg/pubring.gpg
-----------------------------
pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
uid                  subZraw (This ain't Jim Beam) <subZraw@para
bing.com>
sub   2048R/6A85AB25 2011-03-12

pub   1024D/135EA668 2001-03-05
uid                  Richard Stallman (Chief GNUisance) <rms@gnu.
org>
sub   1024g/B1B10ED6 2001-03-05
sub0@opensuse:~>
```

Άψογα! Δείτε τώρα και την απόπειρα εισαγωγής ενός δημοσίου κλειδιού το οποίο όμως –Κύριος οίδε γιατί– έχει ανακληθεί:

```
sub0@opensuse:~> gpg --search-keys cvar@dolnet.gr
gpg: searching for "cvar@dolnet.gr" from hkp server keys.gnupg.net
(1)     Christos Varelas <cvar@dolnet.gr>
          1024 bit DSA key DACC8632, created: 2000-12-04 (revoked)
Keys 1-1 of 1 for "cvar@dolnet.gr".  Enter number(s), N)ext, or Q)
uit > Q
sub0@opensuse:~>
```

Βλέπουμε ότι το κλειδί δημιουργήθηκε περί τα τέλη του 2000 κι ότι για κάποιο λόγο ανακλήθηκε, επομένως δεν έχει κανένα απολύτως νόημα να το εισαγάγουμε

στο public keyring μας. Δεν βαριέσαι, η ζωή συνεχίζεται.

ΑΝΑΚΛΗΣΗ ΚΛΕΙΔΙΟΥ

Όπως συζητήσαμε πρίν λίγο, υπάρχουν λόγοι για τους οποίους ενδέχεται να θέλουμε ν' ανακαλέσουμε ένα δημόσιο κλειδί μας. Προκειμένου να δούμε πώς ακριβώς το πετυχαίνουμε, ας παρακολουθήσουμε το παράδειγμα ανάκλησης του δημοσίου κλειδιού ενός χρήστη με όνομα Chris Vee, διεύθυνση αλληλογραφίας cvarelas@freemail.gr, ID το F4ADE47F και πιστοποιητικό ανάκλησης το chrisVee.asc.

Ξεκινάμε με την εισαγωγή του πιστοποιητικού ανάκλησης:

```
sub0@opensuse:~> gpg --import chrisVee.asc
gpg: key F4ADE47F: "Chris Vee (Free, free, set them free) <cvare
las@freemail.gr>" revocation certificate imported
gpg: Total number processed: 1
gpg:    new key revocations: 1
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f,
2u
```

Αυτό έχει ως αποτέλεσμα την αυτόματη ανάκληση του αντίστοιχου δημοσίου κλειδιού. Όμως γι' την εξέλιξη αυτή οφείλουμε να ενημερώσουμε και τον public keyserver που χρησιμοποιούμε:

```
sub0@opensuse:~> gpg --send-keys F46E7EFF
gpg: sending key F4ADE47F to hkp server keys.gnupg.net
```

Στο εξής, όποιος ψάχνει για το δημόσιο κλειδί του χρήστη με διεύθυνση e-mail cvarelas@freemail.gr, θα βλέπει ότι έχει ανακληθεί κι έτσι δεν θα το χρησιμοποιεί:

```
sub0@opensuse:~> gpg --search-keys cvarelas@freemail.gr
gpg: searching for "cvarelas@freemail.gr" from hkp server keys.
gnupg.net
(1)     Chris Vee (Free, free, set them free) <cvarelas@freemail.
gr>
          2048 bit RSA key F4ADE47F, created: 2011-03-13 (revoked)
Keys 1-1 of 1 for "cvarelas@freemail.gr".  Enter number(s), N)ext,
or Q)uit > Q
sub0@opensuse:~>
```

Και μετά την επιτυχή ανάκληση του κλειδιού, δεν υπάρχει λόγος να κρατάμε το

αντίστοιχο keypair. Διαγράφουμε, λοιπόν, πρώτα το ιδιωτικό και μετά το αντίστοιχο δημόσιο κλειδί:

```
sub0@opensuse:~> gpg --delete-secret-key F4ADE47F
gpg (GnuPG) 2.0.16; Copyright (C) 2009 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

sec  2048R/F4ADE47F 2011-03-13 Chris Vee (Free, free, set them
free) <cvarelas@freemail.gr>

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y

sub0@opensuse:~> gpg --delete-key F4ADE47F
gpg (GnuPG) 2.0.16; Copyright (C) 2009 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

pub  2048R/F4ADE47F 2011-03-13 Chris Vee (Free, free, set them
free) <cvarelas@freemail.gr>

Delete this key from the keyring? (y/N) y
sub0@opensuse:~>
```

Πάνε τα κλειδιά, δεν θα τα ξαναδούμε ποτέ :¦

ΕΞΑΓΩΓΕΣ ΚΑΙ ΕΙΣΑΓΩΓΕΣ ΔΗΜΟΣΙΩΝ ΚΛΕΙΔΙΩΝ

Όπως είπαμε πριν, αν επικοινωνούμε κρυπτογραφημένα μόνο με συγκεκριμένους χρήστες τότε μπορούμε ν' ανταλλάξουμε δημόσια κλειδιά χωρίς τη διαμεσολάβηση keyserver. Ας δούμε πώς, ξεκινώντας με την εξαγωγή του δικού μας δημοσίου κλειδιού από το public keyring μας. Κατά τα γνωστά, αρχικά χρειαζόμαστε το ID του δημοσίου κλειδιού:

```
sub0@opensuse:~> gpg --list-keys
/home/sub0/.gnupg/pubring.gpg
-----------------------------
pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
uid                  subZraw (This ain't Jim Beam) <subZraw@para
```

```
bing.com>
sub   2048R/6A85AB25 2011-03-12

pub   1024D/135EA668 2001-03-05
uid                  Richard Stallman (Chief GNUisance) <rms@gnu.
org>
sub   1024g/B1B10ED6 2001-03-05

pub   2048R/5B17EF55 2011-03-13
uid                  Christos Varelas (We bear gifts) <christos.
varelas@defiant.gr>
uid                  Christos Varelas (Bring the Defiant about)
<cvar@defiant.gr>
uid                  Christos Varelas (We scare because we care)
<cvarelas@gmail.com>
sub   2048R/BCBB10FD 2011-03-13
sub0@opensuse:~>
```

(Όπως βλέπετε από το αποτέλεσμα της εντολής, το public keyring μας έχει πλέον διευρυνθεί.) Στη συνέχεια εξάγουμε το δημόσιο κλειδί σε μορφή ASCII και το αποθηκεύουμε σ' ένα αρχείο με αντιπροσωπευτικό όνομα, π.χ., subZraw.asc:

```
sub0@opensuse:~> gpg --armor --output subZraw.asc --export EB-
DCE7DA
sub0@opensuse:~> cat subZraw.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.16 (GNU/Linux)

mQENBE17k9cBCACxxFy0NOFJXR+wDd8rWUfRDhlNu8fIxnma8cnNFNIPpAvqN47O
EW/vr0n8vHtQN94w0BnQSxdyd8ukSuAYGARISvhhDiQVjCmvQVedPJwxi0YxqVHf
AHMs2nHsVROItvaeMxio+OZtZx/6iRu0CjL5t9N8sd75tvUQpb+jp97yLA4JY0Su
qt8/oAoby/dTuShbJUDmOoTyB+1Xs1jW39Xuqj9NxLteXYUq/WvUy225glg+zpLf
4TFgkCxHAzIhbuXDoV6h0c22/FraXE3ATZAwCbu+IC5LCyixJHkvHoVZPUiotwv/
...
sMc3PSswU4OkWnkwAYH+chehRamUR8hC3t4fr4Bl6GNe3ZAMvhDS9RGJ9TXPbaRP
vo/bxclMIQzYH+FuK4RSjzqGsRWVsWpS+La/8kDLMn/2GkxN0ktFxoHkQpUVVlvv
x3qLlLY9BVrCRDGBb4XPxXPFLsjDYQXqpb2qtLP4cjT7ItF4qcQ9K2Kcb3pRkGDr
9q5SLgf2OoQtCzK4a7zkPnFOWKY8o7ol9LFpGye1gBuY3WZSJYGq7At0aIxWqMUw
QFkKGFriWRskvFytE2RoMPYoTvSA26pIeQQPYw==
=YRTB
-----END PGP PUBLIC KEY BLOCK-----
sub0@opensuse:~>
```

Άψογα, το κλειδί μας είναι *και* ωραίο :) Το αρχείο subZraw.asc μπορούμε να το δώσουμε σ' όποιους χρήστες θέλουμε. Εναλλακτικά, μπορούμε να το δημοσιεύσουμε στο site μας ή να το χρησιμοποιούμε ως υπογραφή στα mail που στέλνουμε. Και πώς το ενσωματτώνει κάποιος ενδιαφερόμενος στο public keyring του; Αρκετά απλά. Αν μάλιστα το επιθυμεί, μπορεί να κάνει κι έξτρα ελέγχους, ώστε να διαπιστώσει ότι το νέο δημόσιο κλειδί πράγματι ανήκει σ' εκείνον που υποτίθεται ότι ανήκει. Δείτε, π.χ., πώς ο χρήστης με username cvar εισάγει στο Mac OS X του το δημόσιο κλειδί subZraw.asc:

```
imac24:~ cvar$ gpg --import subZraw.asc
gpg: key EBDCE7DA: public key "subZraw (Underworld SA) <subZraw@
defiant.gr>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)

imac24:~ cvar$ gpg --list-keys
/Users/cvar/.gnupg/pubring.gpg
------------------------------
pub   2048R/5B17EF55 2011-03-13
uid                  Christos Varelas (We bear gifts) <christos.
varelas@defiant.gr>
uid                  Christos Varelas (We scare because we care)
<cvarelas@gmail.com>
uid                  Christos Varelas (Bring the Defiant about)
<cvar@defiant.gr>
sub   2048R/BCBB10FD 2011-03-13

pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
uid                  subZraw (This ain't Jim Beam) <subZraw@para
bing.com>
sub   2048R/6A85AB25 2011-03-12
```

Αν τώρα ο cvar θέλει να βεβειωθεί για το κλειδί που μόλις εισήγαγε, μπορεί να επικοινωνήσει, π.χ., μ' ένα απλό τηλεφώνημα, με τον ίδιο τον sub0 και να του ζητήσει το αποτύπωμα (fingerprint) του κλειδιού του. (Το αποτύπωμα επιστρέφεται από την εντολή fpr του interactive environment του gpg.) Στη συνέχεια θα συγκρίνει το αποτύπωμα που πήρε με το αποτέλεσμα της εντολής fpr στο δικό του υπολογιστή κι αν δει ότι συμπίπτουν, θα προχωρήσει στην υπογραφή του νέου κλειδιού:

```
imac24:~ cvar$ gpg --edit-key EBDCE7DA
```

```
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

pub  2048R/EBDCE7DA  created: 2011-03-12  expires: never      us-
age: SC
                     trust: unknown       validity: unknown
sub  2048R/6A85AB25  created: 2011-03-12  expires: never      us-
age: E
[ unknown] (1). subZraw (Underworld SA) <subZraw@defiant.gr>
[ unknown] (2)  subZraw (This ain't Jim Beam) <subZraw@parabing.
com>

gpg> fpr
pub   2048R/EBDCE7DA 2011-03-12 subZraw (Underworld SA) <subZraw@
defiant.gr>
 Primary key fingerprint: A34A B306 90A3 A042 61F6  163F 2B57 FA04
EBDC E7DA

gpg> sign
Really sign all user IDs? (y/N) y

pub  2048R/EBDCE7DA  created: 2011-03-12  expires: never      us-
age: SC
                     trust: unknown       validity: unknown
 Primary key fingerprint: A34A B306 90A3 A042 61F6  163F 2B57 FA04
EBDC E7DA
     subZraw (Underworld SA) <subZraw@defiant.gr>
     subZraw (This ain't Jim Beam) <subZraw@parabing.com>

Are you sure that you want to sign this key with your
key "Christos Varelas (We bear gifts) <christos.varelas@defiant.
gr>" (5B17EF55)

Really sign? (y/N) y

You need a passphrase to unlock the secret key for
user: "Christos Varelas (We bear gifts) <christos.varelas@defiant.
gr>"
2048-bit RSA key, ID 5B17EF55, created 2011-03-13
```

```
gpg> check
uid  subZraw (Underworld SA) <subZraw@defiant.gr>
sig!3        EBDCE7DA 2011-03-12  [self-signature]
sig!         5B17EF55 2011-03-13  Christos Varelas (We bear gifts)
<christos.var
uid  subZraw (This ain't Jim Beam) <subZraw@parabing.com>
sig!3        EBDCE7DA 2011-03-12  [self-signature]
sig!         5B17EF55 2011-03-13  Christos Varelas (We bear gifts)
<christos.var

gpg> quit
Save changes? (y/N) y
imac24:~ cvar$
```

Φυσικά, για να μπορέσει να υπογράψει ο cvar έδωσε το passphrase του ιδιωτικού του κλειδιού.

ΕΞΑΓΩΓΕΣ ΚΑΙ ΕΙΣΑΓΩΓΕΣ ΙΔΙΩΤΙΚΩΝ ΚΛΕΙΔΙΩΝ

Το keypair που έχουμε φτιάξει σ ' ένα συγκεκριμένο υπολογιστή ή λειτουργικό σύστημα είναι πολύ πιθανό να το θέλουμε και σε κάποιον άλλον υπολογιστή ή λειτουργικό. Πέρα από το δημόσιο κλειδί, λοιπόν, πρέπει να δούμε πώς εξαγάγουμε και εισαγάγουμε *και* το ιδιωτικό. Ως ένα παράδειγμα που επιδεικνύει την όλη διαδικασία, θα παρακολουθήσουμε πρώτα την εξαγωγή του ιδιωτικού κλειδιού του subZraw, το οποίο διατηρείται στο user account με όνομα sub0, στον υπολογιστή με το openSUSE. Ακολούθως θα δούμε πώς το ίδιο ιδιωτικό κλειδί εισαγάγεται στο private keyring του Christos Varelas, το οποίο βρίσκεται στο user account με όνομα cvar ενός υπολογιστή με Mac OS X.

Ξεκινάμε με την εξαγωγή:

```
sub0@opensuse:~> gpg --list-secret-keys
/home/sub0/.gnupg/secring.gpg
-----------------------------
sec   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (This ain't Jim Beam) <subZraw@para-
bing.com>
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
ssb   2048R/6A85AB25 2011-03-12

sub0@opensuse:~> gpg --armor --output subZraw-private.asc --ex
port-secret-key EBDCE7DA
```

```
sub0@opensuse:~> cat subZraw-private.asc
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v2.0.16 (GNU/Linux)

lQO+BE17k9cBCACxxFy0NOFJXR+wDd8rWUfRDhlNu8fIxnma8cnNFNIPpAvqN47O
EW/vr0n8vHtQN94w0BnQSxdyd8ukSuAYGARISvhhDiQVjCmvQVedPJwxi0YxqVHf
...
5D5xTlimPKO6NfSxaRsntYAbmN1mUiWBquwLdGiMVqjFMEBZChha4lkbJLxcrRNk
aDD2KE70gNuqSHkED2M=
=3K5s
-----END PGP PRIVATE KEY BLOCK-----
sub0@opensuse:~>
```

Τώρα, με κάποιον ασφαλή τρόπο ο sub0 πρέπει να στείλει στον cvar το ιδιωτικό του κλειδί – στο παράδειγμά μας το αρχείο subZraw-private.asc. Ένας τρόπος για να το πετύχει είναι να το κρυπτογραφήσει με το δημόσιο κλειδί του cvar και μετά να του το στείλει ως συνημμένο σε e-mail. Εναλλακτικά, αν υπάρχει δυνατότητα μπορεί να του το στείλει μέσω SSH. Όπως και να 'χει, υποθέτουμε ότι το αρχείο subZraw-private.asc φτάνει στο λογαριασμό του cvar. Ας δούμε πώς το εισαγάγει στο private keyring του:

```
imac24:~ cvar$ gpg --import subZraw-private.asc
gpg: key EBDCE7DA: secret key imported
gpg: key EBDCE7DA: "subZraw (Underworld SA) <subZraw@defiant.gr>"
not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
imac24:~ cvar$
```

(Το δεύτερο μήνυμα που επιστρέφει το gpg στο παράδειγμά μας οφείλεται στο γεγονός ότι στο public keyring του Christos Varelas είναι ήδη εισηγμένο το δημόσιο κλειδί του subZraw.) Πριν την εισαγωγή του subZraw-private.asc, το private keyring του Christos Varelas ήταν το ακόλουθο:

```
imac24:~ cvar$ gpg --list-secret-keys
/Users/cvar/.gnupg/secring.gpg
------------------------------
sec   2048R/5B17EF55 2011-03-13
uid                  Christos Varelas (We scare because we care)
<cvarelas@gmail.com>
```

```
uid                  Christos Varelas (Bring the Defiant about)
<cvar@defiant.gr>
uid                  Christos Varelas (We bear gifts) <christos.
varelas@defiant.gr>
ssb   2048R/BCBB10FD 2011-03-13
```

Τώρα, μετά την εισαγωγή του νέου ιδιωτικού κλειδιού, το ίδιο private keyring έχει ως ακολούθως:

```
imac24:~ cvar$ gpg --list-secret-keys
/Users/cvar/.gnupg/secring.gpg
------------------------------
sec   2048R/5B17EF55 2011-03-13
uid                  Christos Varelas (We scare because we care)
<cvarelas@gmail.com>
uid                  Christos Varelas (Bring the Defiant about)
<cvar@defiant.gr>
uid                  Christos Varelas (We bear gifts) <christos.
varelas@defiant.gr>
ssb   2048R/BCBB10FD 2011-03-13

sec   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (This ain't Jim Beam) <subZraw@para
bing.com>
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
ssb   2048R/6A85AB25 2011-03-12
imac24:~ cvar$
```

Όλα καλά κι ωραία.

ΔΙΑΓΡΑΦΗ ΔΗΜΟΣΙΟΥ Η/ΚΑΙ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ

Για οποιονδήποτε λόγο ενδέχεται να θέλουμε τη διαγραφή ενός δημοσίου κλειδιού από το keyring μας. Αυτή επιτυγχάνεται εύκολα κι ο ακριβής τρόπος φαίνεται στο ακόλουθο παράδειγμα, όπου από το keyring του subZraw διαγράφουμε το δημόσιο κλειδί του Richard Stallman:

```
sub0@opensuse:~> gpg --list-keys
/home/sub0/.gnupg/pubring.gpg
-----------------------------
pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
uid                  subZraw (This ain't Jim Beam) <subZraw@para
```

```
bing.com>
sub   2048R/6A85AB25 2011-03-12

pub   1024D/135EA668 2001-03-05
uid                  Richard Stallman (Chief GNUisance) <rms@gnu.
org>
sub   1024g/B1B10ED6 2001-03-05

pub   2048R/5B17EF55 2011-03-13
uid                  Christos Varelas (We bear gifts) <christos.
varelas@defiant.gr>
uid                  Christos Varelas (Bring the Defiant about)
<cvar@defiant.gr>
uid                  Christos Varelas (We scare because we care)
<cvarelas@gmail.com>
sub   2048R/BCBB10FD 2011-03-13

sub0@opensuse:~> gpg --delete-key 135EA668
gpg (GnuPG) 2.0.16; Copyright (C) 2009 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

pub  1024D/135EA668 2001-03-05 Richard Stallman (Chief GNUisance)
<rms@gnu.org>

Delete this key from the keyring? (y/N) y

sub0@opensuse:~> gpg --list-keys
/home/sub0/.gnupg/pubring.gpg
-----------------------------
pub   2048R/EBDCE7DA 2011-03-12
uid                  subZraw (Underworld SA) <subZraw@defiant.gr>
uid                  subZraw (This ain't Jim Beam) <subZraw@para-
bing.com>
sub   2048R/6A85AB25 2011-03-12

pub   2048R/5B17EF55 2011-03-13
uid                  Christos Varelas (We bear gifts) <christos.
varelas@defiant.gr>
uid                  Christos Varelas (Bring the Defiant about)
<cvar@defiant.gr>
```

```
uid                  Christos Varelas (We scare because we care)
<cvarelas@gmail.com>
sub   2048R/BCBB10FD 2011-03-13
sub0@opensuse:~>
```

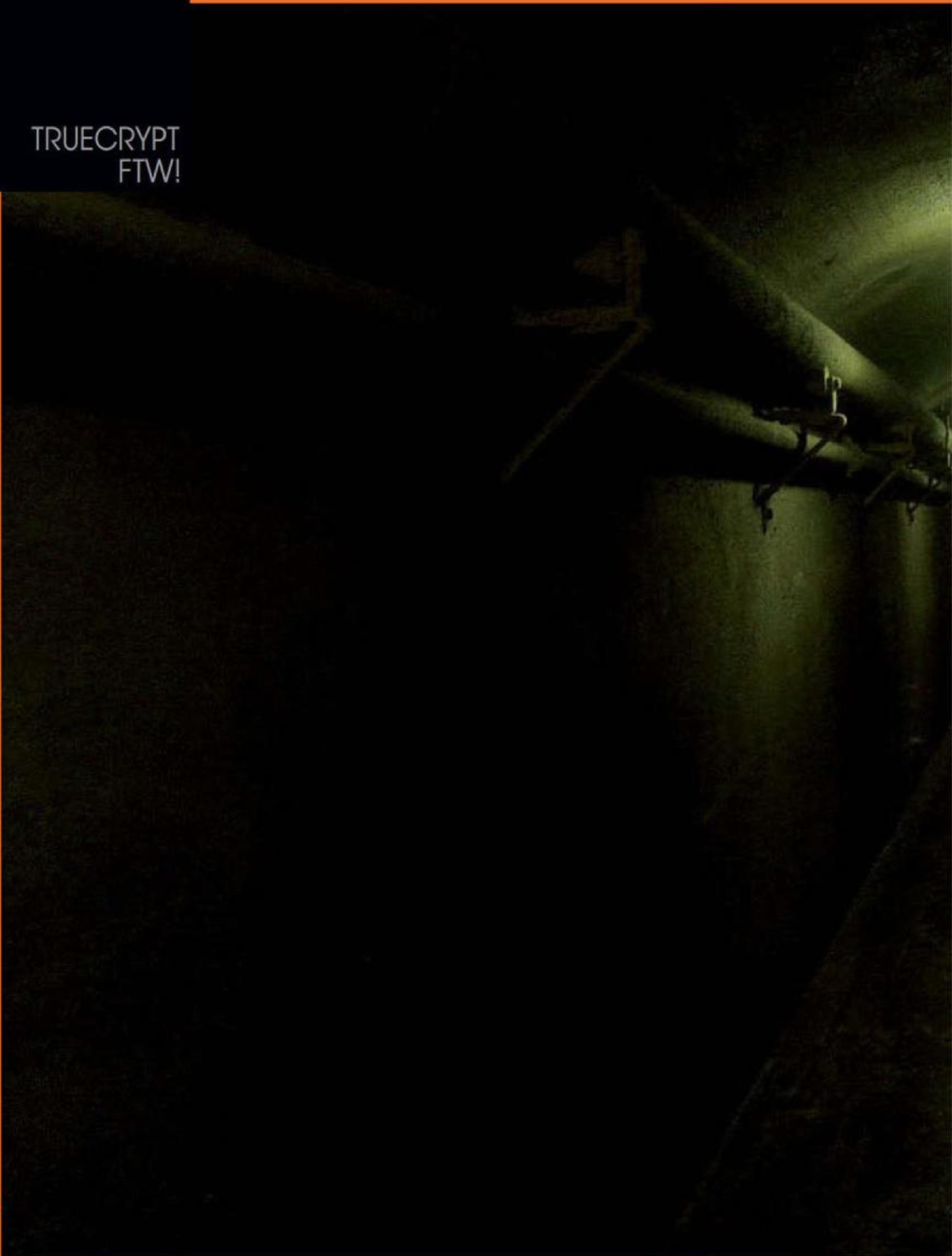
Εντελώς παρόμοια γίνεται και η διαγραφή ιδιωτικών κλειδιών, μόνο που σε μια τέτοια περίπτωση στο gpg δίνουμε την παράμετρο --delete-secret-key (βλ. και παράδειγμα στην ενότητα «Ανάκληση κλειδιού»).

ΤΟ GNUPG ΣΤΗΝ ΠΡΑΞΗ!

Πλέον γνωρίζουμε όλα τα απαραίτητα –και λίγα περισσότερα– γύρω από τη χρήση του GPG, κυρίως όσον αφορά στη διαχείριση των κλειδιών. Στο άρθρο που αρχίζει από τη σελίδα 54 περνάμε σε πρακτικά παραδείγματα, όπου συγκεκριμένα δείχνουμε πώς κρυπτογραφούμε, αποκρυπτογραφούμε και υπογράφουμε mail ή/και αρχεία. Επιπρόσθετα, παρουσιάζουμε κι ορισμένα προγράμματα διαχείρισης για το περιβάλλον γραφικών, τα οποία διευκολύνουν σημαντικά την καθημερινή αλληλεπίδραση με το GPG. Μην περιμένετε λοιπόν άλλο, γυρίστε τώρα στη σελίδα 54!

subZraw

TRUECRYPT FTW!



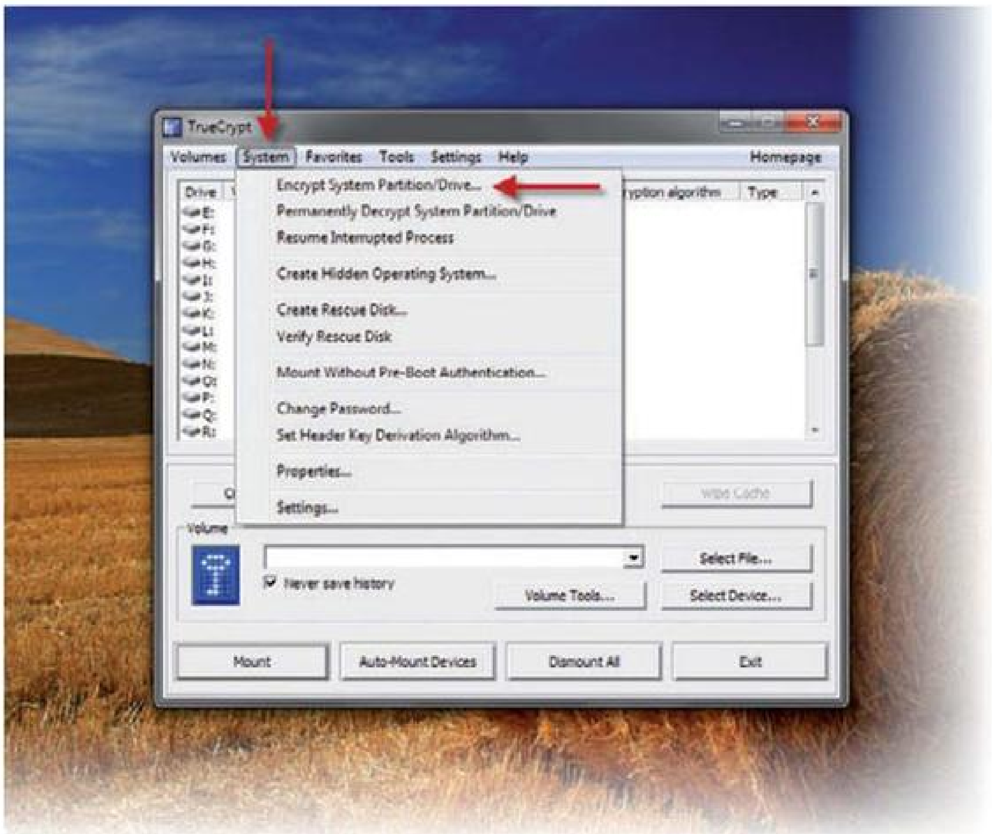
Χάστε το laptop σας, χωρίς άγχος

Τι είναι το χειρότερο που μπορεί να σας συμβεί *μετά* το χάσιμο ή την κλοπή του laptop σας; Μα το γεγονός ότι κάποιοι θ' αποκτήσουν πρόσβαση στα περιεχόμενα του δίσκου του. Φυσικά το ίδιο ισχύει και για τα δεδομένα που βρίσκονται στο δίσκο ή στους δίσκους του PC σας.

ΚΑΛΑ ΚΙ ΑΓΙΑ τα backup της δουλειάς και των πολύτιμων αρχείων μας, όμως υπάρχουν φορές που δεν θέλουμε κανέναν ν' αποκτήσει πρόσβαση στα δεδομένα μας – και δεν χρειάζεται καν να 'ναι αυτό που λέμε «ευαίσθητα» ή «πολύτιμα». Σίγουρα θα 'χει περάσει από το μυαλό σας κάποιο ανάλογο σενάριο, όπου ουσιαστικά χάνετε τον έλεγχο των δεδομένων σας. Θα παραδεχτούμε ευθύς εξαρχής ότι από τη μεριά μας έχουμε μια τάση ν' αποδιώχνουμε τέτοιες και παρόμοιες ανήσυχες σκέψεις, θεωρώντας ότι αυτά είναι ατυχήματα που συμβαίνουν μόνο στους άλλους. Ας το παραδεχτούμε, κάπως έτσι σκεφτόμαστε όλοι μας. Εδώ που τα λέμε, βέβαια, τίποτα δεν μας διασφαλίζει ότι αύριο κιόλας δεν θα βρεθούμε κι εμείς στην ομάδα αυτών των απρόσωπων «άλλων». Ευτυχώς, λύση για το ζήτημα της απώλειας ελέγχου των δεδομένων μας υπάρχει. Είναι μάλιστα 100% αξιόπιστη και –το καλύτερο απ' όλα– εντελώς δωρεάν! Αναφερόμαστε στο TrueCrypt (www.truecrypt.org), για το οποίο μπορείτε να διαβάσετε πολύ περισσότερα στο σχετικό άρθρο μέσα στο RAM που συνοδεύει το total XAKER Απριλίου. (Ναι, εμείς το λέμε έτσι και οι άλλοι, από τη μεριά του RAM, το λένε κάπως διαφορετικά: «...μπορείτε να διαβάσετε στο total XAKER, που συνοδεύει το RAM του τάδε μήνα». Μην το ψάχνετε, το ένα περιοδικό συνοδεύει τ' άλλο :D)
Στο παρόν άρθρο δείχνουμε, αναλυτικά και βήμα προς βήμα, πώς κρυπτογραφούμε το διαμέρισμα ή το δίσκο στον οποίο είναι εγκατεστημένα τα Windows. Πρόκειται για μια δυνατότητα του TrueCrypt που παρέχεται μόνο για το εν λόγω λειτουργικό κι αποτελεί μια άριστη επιλογή ειδικά για τους φορητούς υπολογιστές: Ακόμα κι ολόκληρο το laptop να μας πάρουν, αν δεν γνωρίζουν τον κωδικό αποκρυπτογράφησης, δεν θα μπορέσουν *ποτέ* ν' αποκτήσουν πρόσβαση στα περιεχόμενα του δίσκου – ούτε καν να bootάρουν τα Windows που βρίσκονται πάνω του. Φυσικά, η κρυπτογράφηση του δίσκου/διαμερίσματος συστήματος δεν έχει νόημα μόνο σε Windows laptops αλλά και σε desktop PC. Αλλά γι' αυτό ούτως ή άλλως εσείς κρίνετε, εσείς αποφασίζετε. Πριν δούμε αναλυτικά τη διαδικασία, να σημειώσουμε ότι, παρά την κρυπτογράφηση, δεν θα παρατηρήσετε ουσιαστική πτώση στις επιδόσεις του δίσκου. Πρακτικά, το laptop ή το PC σας θα συμπεριφέρεται όπως πριν την κρυπτογράφηση.

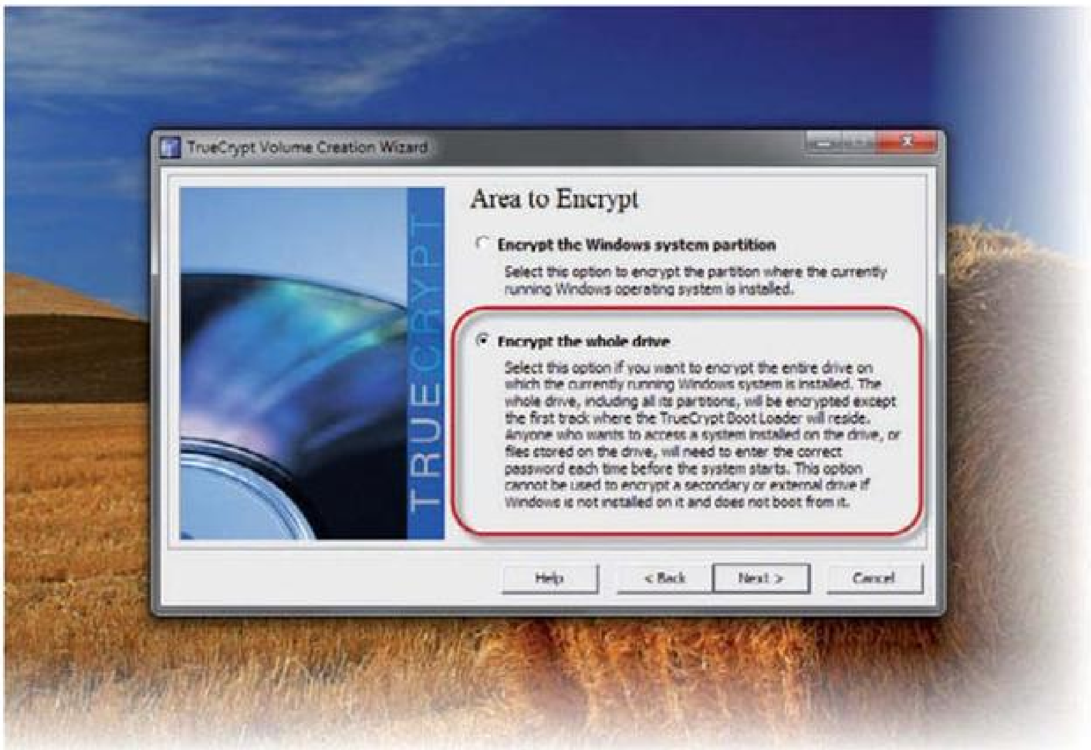
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΙΣΚΟΥ/ ΔΙΑΜΕΡΙΣΜΑΤΟΣ ΣΥΣΤΗΜΑΤΟΣ

Η μόνη ερώτηση του installer στην οποία οφείλουμε να δώσουμε ιδιαίτερη προσοχή: Θέλουμε το TrueCrypt εγκατεστημένο στο σύστημα κι όχι αυτόνομο, στο δικό του φάκελο.

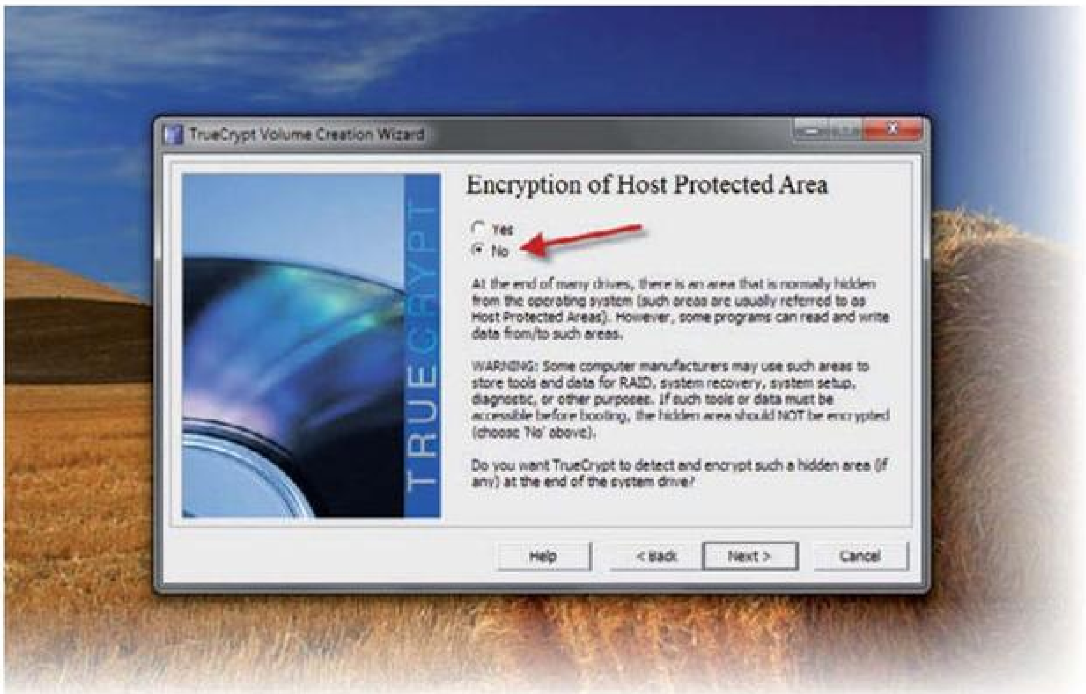


Μετά την εγκατάσταση, τρέχουμε το TrueCrypt και για την κρυπτογράφηση του system partition επιλέγουμε System --> Encrypt System Partition/Drive. Προφανές, αλλά για λόγους πληρότητας είπαμε να το αναφέρουμε ;)

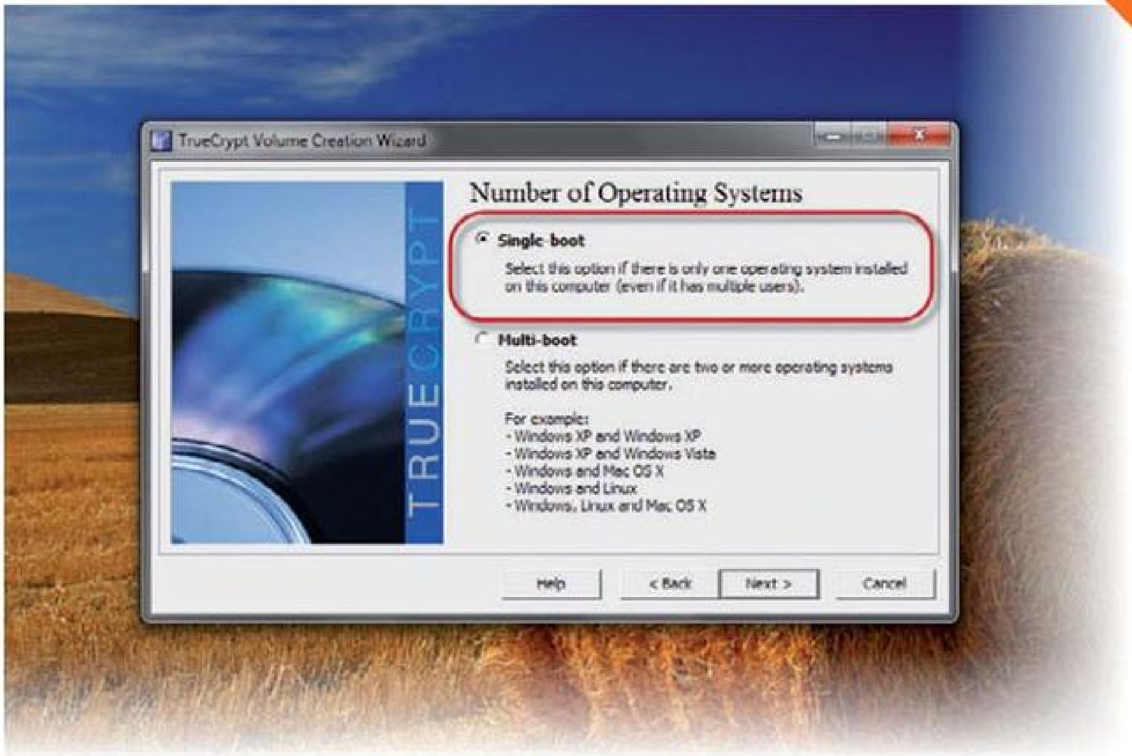
Δεν ξέρουμε για 'σας, όμως εμάς το θέμα του plausible deniability δεν μας απασχολεί. Αν δηλαδή μας γραπώσουν και με τρομακτικές απειλές μας αποσπάσουν τον κωδικό που προστατεύει την κρυπτογραφημένη κατάτμηση των Windows, ε, θα τους τον δώσουμε και τα δεδομένα μας χαλάλι τους. Γι' αυτό και στην ερώτηση περί του type of system encryption επιλέγουμε το normal. Σε αντίθετη περίπτωση, το TrueCrypt θα δημιουργούσε ένα κρυμμένο διαμέρισμα με το λειτουργικό του σύστημα, η ύπαρξη του οποίου δεν θα είναι εύκολο ν' αποδειχθεί.



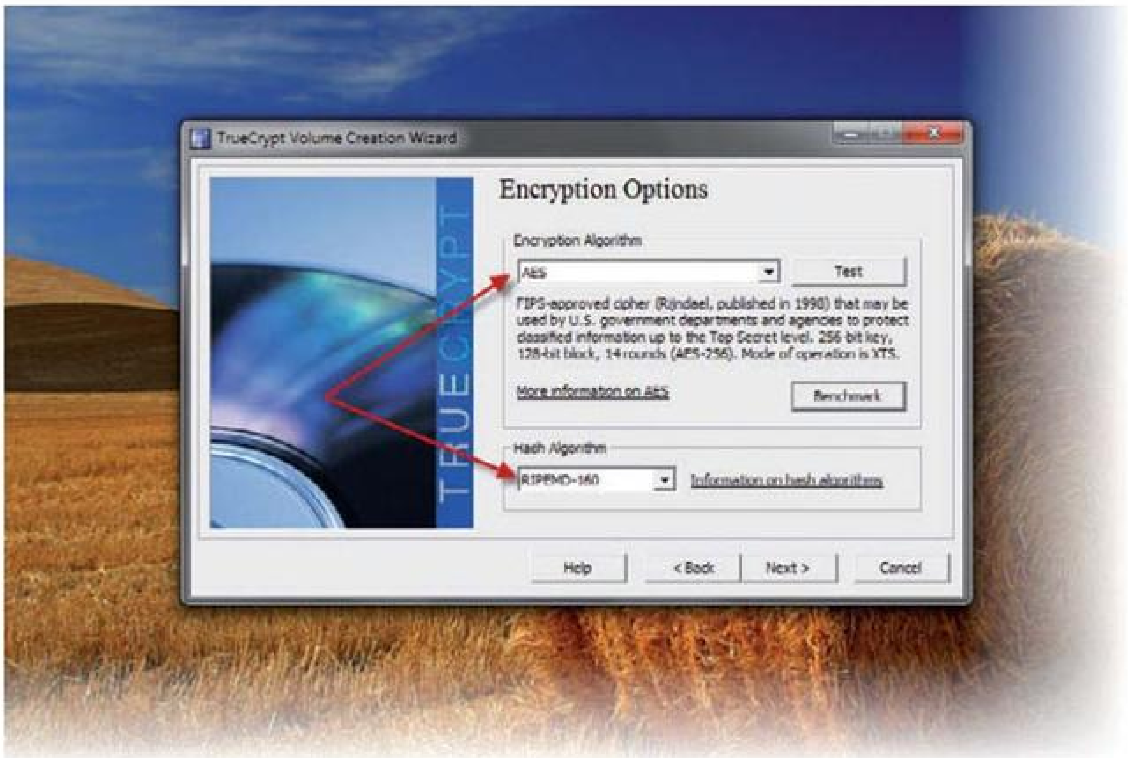
Στο μηχάνημα των δοκιμών μας το λειτουργικό καταλάμβανε ολόκληρο το δίσκο. Επιλέξαμε, λοιπόν, την κρυπτογράφηση ολόκληρου του δίσκου.



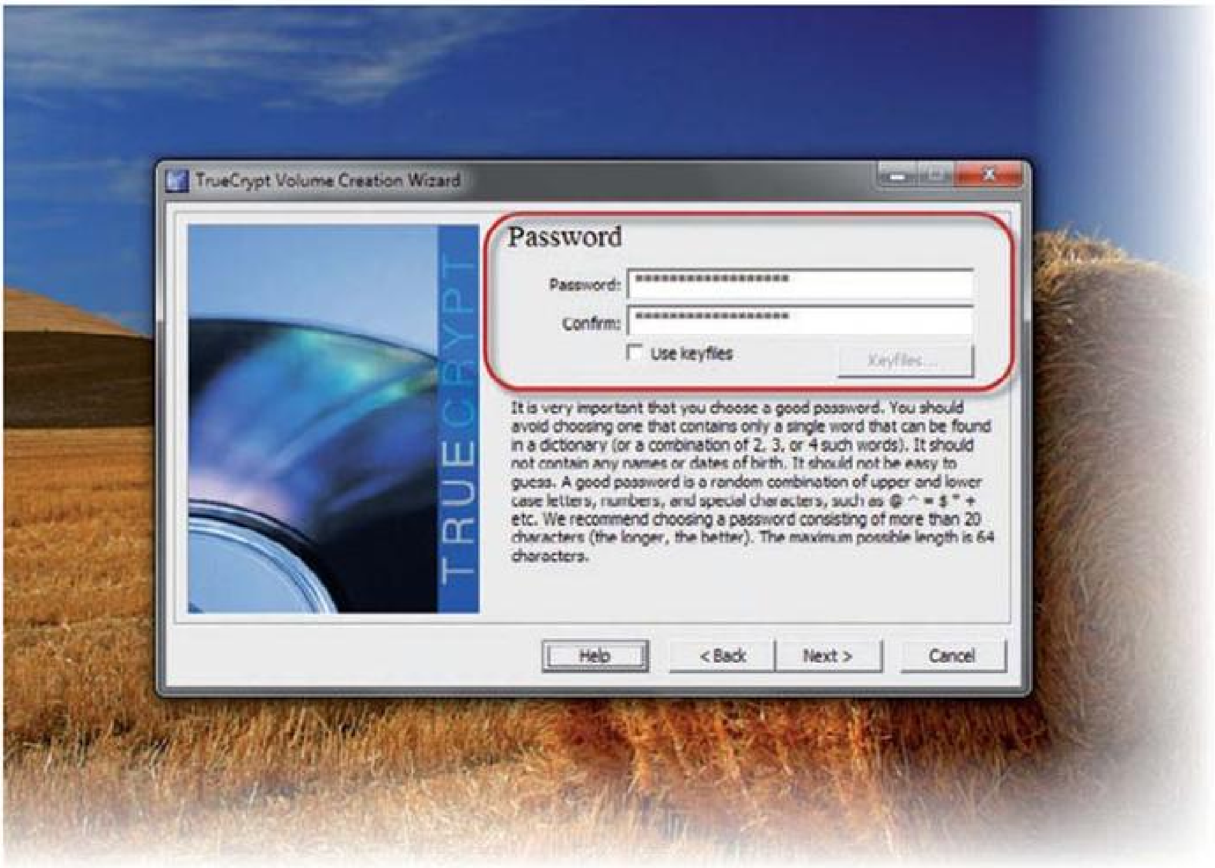
Οι δίσκοι κάποιων laptop έρχονται με δύο διαμερίσματα. Στο μικρότερο είναι αποθηκευμένα ορισμένα εργαλεία κι οδηγοί – ενδεχομένως κι ένα image του λειτουργικού, το οποίο χρησιμοποιείται όταν ζητείται η επαναφορά του υπολογιστή στις εργοστασιακές ρυθμίσεις. Αν ο δίσκος του laptop σας έχει ένα τέτοιο διαμέρισμα, ίσως δεν είναι καλή ιδέα να το κρυπτογραφήσετε: Πιθανόν ορισμένα εργαλεία κι οδηγοί που βρίσκονται εκεί ν' αναζητούνται πριν ακόμα αρχίσει η κανονική εκκίνηση του λειτουργικού.



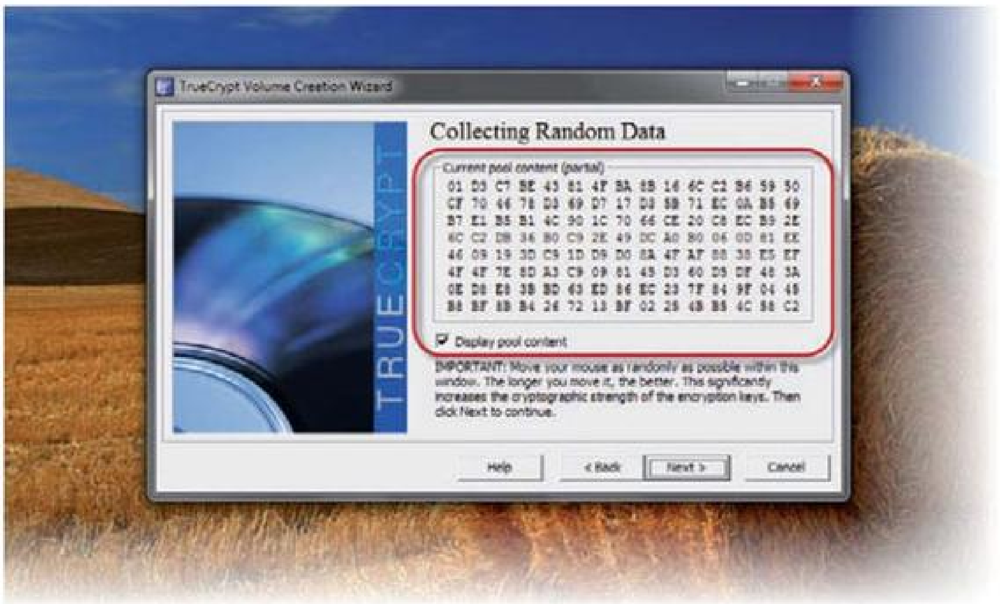
Έχετε ένα ή περισσότερα λειτουργικά συστήματα εγκατεστημένα στον υπολογιστή σας; Επιλέξτε αναλόγως.



Λεπτομέρειες για τον αλγόριθμο κρυπτογράφησης. Αφήστε τις προεπιλογές. Είναι ο καλύτερος συμβιβασμός μεταξύ ασφάλειας και ταχύτητας.



Είναι ώρα να ορίσουμε τον κωδικό που θα απαιτείται για την αποκρυπτογράφηση της κατάτμησης συστήματος, ώστε να είναι δυνατή η εκκίνηση των Windows. Προσοχή: Επιλέξτε έναν καλό κωδικό, ο οποίος δεν θα προέρχεται από κάποια λέξη που υπάρχει σε λεξικό και θ' αποτελείται από ένα συνδυασμό πεζών, κεφαλαίων, αριθμών και συμβόλων. Επιπρόσθετα, το TrueCrypt προτείνει να 'χει μήκος τουλάχιστον 20 χαρακτήρες. Φυσικά, περιττό να σημειώσουμε ότι ο κωδικός πρέπει να 'ναι έτσι επιλεγμένος ώστε να τον θυμόσαστε εύκολα και να μην υπάρχει περίπτωση να τον ξεχάσετε. Ένα τρικ που μπορείτε να εφαρμόσετε είναι να πάρετε ορισμένες λέξεις από τους στίχους ενός αγαπημένου σας τραγουδιού, να τις βάλετε στη σειρά, ορισμένα γράμματα να τα γυρίσετε κεφαλαία και να κάνετε κι αντικαταστάσεις του στιλ a --> @, e --> 3, i --> l κ.λπ. Πάντως, στην περίπτωση που όντως ξεχάσετε τον κωδικό σας και δεν μπορείτε με τίποτα να τον θυμηθήτε, τότε η πιθανότητα αποκρυπτογράφησης είναι ίση με την πιθανότητα να κάνετε ταξίδι στο παρελθόν, να αλληλεπιδράσετε με πέντε σημαντικές ιστορικές φυσιογνωμίες και να μην προκαλέσετε την παραμικρή διαταραχή στο timeline.



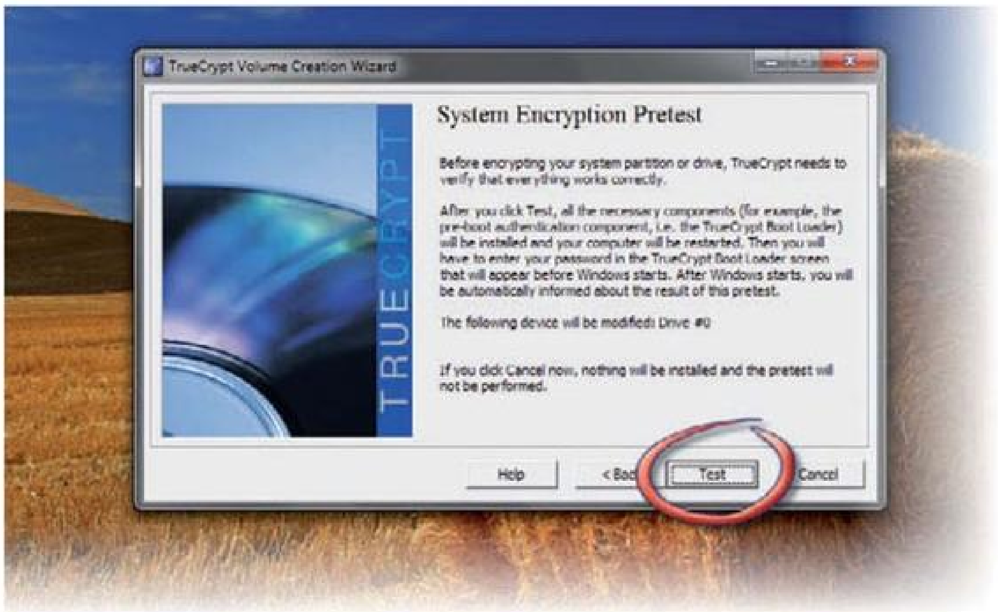
Η δημιουργία καλών κλειδιών κρυπτογράφησης εξαρτάται από το λεγόμενο random seed, που δεν είναι τίποτε άλλο από μια ακολουθία τυχαίων αριθμών. Έχετε υπόψη ότι οι αλγόριθμοι παραγωγής τυχαίων αριθμών ουσιαστικά δίνουν τους λεγόμενους ψευδοτυχαίους αριθμούς, δηλαδή αριθμούς που *δεν* παράγονται με τυχαίο τρόπο. Μπορεί να δείχνουν ότι είναι τυχαία επιλεγμένοι, στην πραγματικότητα όμως έχουν προκύψει από μια σαφώς ορισμένη, ντετερμινιστική διαδικασία. Γι' αυτό και το TrueCrypt ζητά τη βοήθειά σας, προτείνοντας να κινήσετε για λίγη ώρα τυχαία το ποντίκι πάνω από το πλαίσιο Current pool content. Μπορείτε να σκέφτεστε ότι την τυχαία κίνηση του χεριού το πρόγραμμα τη μεταφράζει σε τυχαίους αριθμούς. Αφού, λοιπόν, ξεχεριαστείτε για μερικά δευτερόλεπτα, κάντε ένα κλικ στο κουμπί Next.

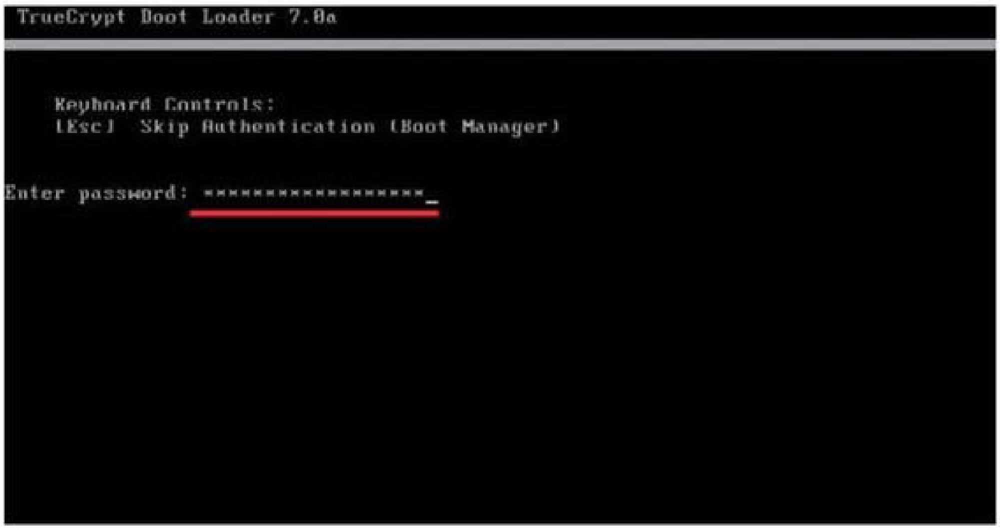
Πριν την ίδια την κρυπτογράφηση του διαμερίσματος ή του δίσκου συστήματος, το TrueCrypt προτείνει τη δημιουργία ενός CD ή DVD εκτάκτου ανάγκης. Αυτό θα φανεί πολύτιμο αν, π.χ., καταστραφεί ο boot loader του TrueCrypt και δεν μπορείτε να προχωρήσετε στην αποκρυπτογράφηση και στην εκκίνηση του λειτουργικού. Μια άλλη περίπτωση που θα χρειαστεί είναι αν πάθει ζημιά η εγκατάσταση των Windows και δεν μπορούν να εκκινήσουν, όπου τότε θα 'χετε την επιλογή να αποκρυπτογραφήσετε *μόνιμα* τον αντίστοιχο δίσκο ή διαμέρισμα, συνεπώς ν' αποκτήσετε πλήρη πρόσβαση στα δεδομένα του βάζοντας το δίσκο σ' ένα άλλο μηχάνημα ή απλά εκινώντας το ίδιο από ένα Linux live CD. Τέλος, το CD/DVD εκτάκτου ανάγκης θα έχει κι ένα αντίγραφο του πρώτου track του δίσκου *πριν* την κρυπτογράφηση, για την περίπτωση που χρειαστεί να το επαναφέρετε. Το ISO image την CD/DVD εκκίνησης το TrueCrypt θα το δημιουργήσει σε όποια θέση του υποδείξουμε.

Το TrueCrypt γράφει τα ISO που δημιουργεί με τη βοήθεια του εργαλείου Disc Image Burner των Windows. Δεν μπορείτε να προσπεράσετε αυτό το στάδιο – και δεν έχει καμία σημασία αν βαριόσαστε :) Πριν συνεχίσει το TrueCrypt τη δουλειά του, οφείλετε να βάλετε στον οδηγό ένα άδειο CD ή DVD και να γράψετε το image. Μετά την εγγραφή, το TrueCrypt θα απαιτήσει και την επαλήθευση του μέσου. Όταν τελειώσουν οι εργασίες με το CD/DVD, καλό είναι να το φυλλάξετε σ' ένα ασφαλές μέρος.

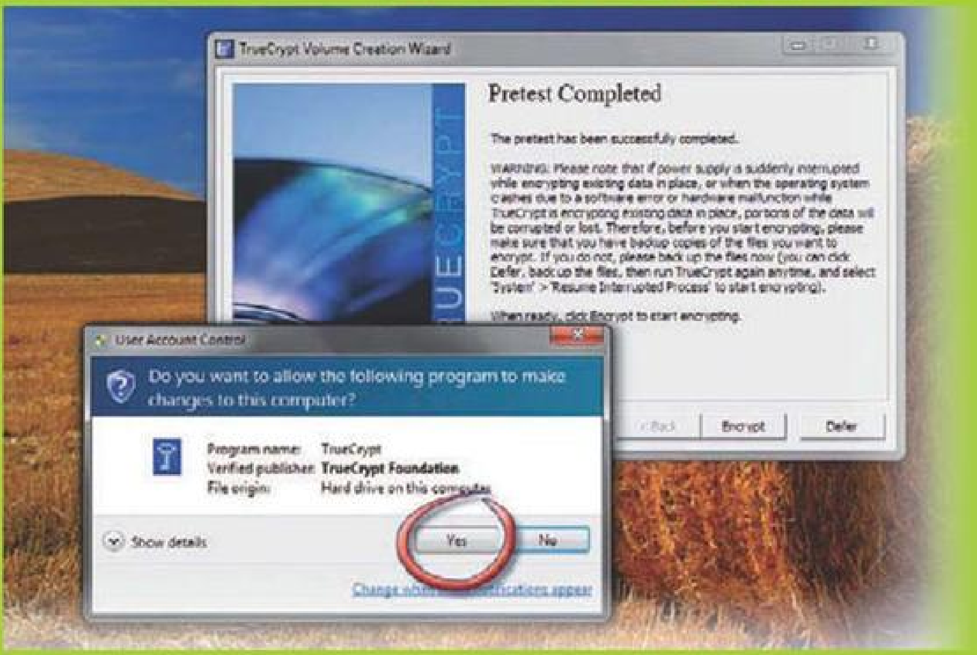
Όσο απίθανο κι αν φαντάζει, δεδομένα σε δίσκους που έχουν γραφτεί από πάνω με άλλα δεδομένα, είναι δυνατόν ν' ανακτηθούν. Σίγουρα δεν είναι το πιο εύκολο πράγμα στον κόσμο, υπάρχουν ωστόσο τεχνικές που κάποια αποφασισμένη υπηρεσία θα μπορούσε να εφαρμόσει ώστε να το πετύχει. Η ανάκτηση όμως γίνεται πρακτικά αδύνατη όταν πάνω από τα αρχικά δεδομένα έχουν ήδη γραφτεί συνδυασμοί συγκεκριμένων και ψευδοτυχαίων δεδομένων περισσότερες από μία φορές. Αν τώρα εσείς έχετε λόγο να πιστεύετε ότι κάποιος, κάπου, θα πάρει τον κρυπτογραφημένο σας δίσκο και θα εφαρμόσει φοβερές και τρομερές τεχνικές με στόχο την ανάκτηση των μη κρυπτογραφημένων τομέων του (tracks), τότε μπορείτε να ζητήσετε από το TrueCrypt *πριν* αντικαταστήσει τους τομείς με τις κρυπτογραφημένες τους εκδοχές να γράψει από πάνω τους δεδομένα για ένα συγκεκριμένο αριθμό φορών. Σημειώστε πως, αν αποφασίσετε να το κάνετε, τότε ο χρόνος που θα απαιτηθεί για την κρυπτογράφηση του δίσκου ή του διαμερίσματος θα αυξηθεί σημαντικά. Εμείς πάντως σκεφτήκαμε ότι αν κάποια υπηρεσία πάρει τον κρυπτογραφημένο μας δίσκο και με χρήση πανάκριβου εξοπλισμού καταφέρει ν' ανακτήσει τα μη κρυπτογραφημένα του δεδομένα, τότε χαλάλι της ;)

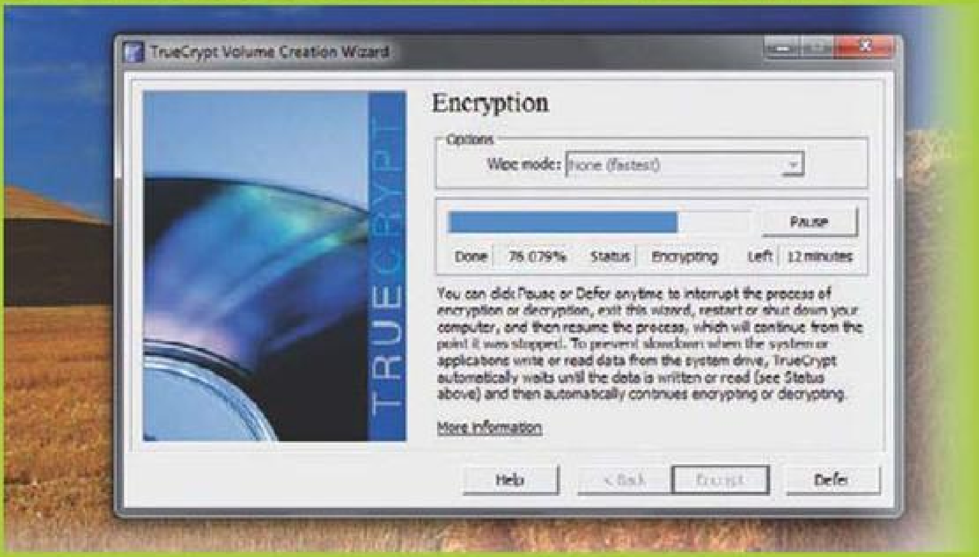
Στη συνέχεια, το TrueCrypt θέλει να κάνει μια δοκιμή, ώστε να διαπιστώσει αν ο δικός του boot loader, καθώς και ο μηχανισμός εισαγωγή του κωδικού αποκρυπτογράφησης, λειτουργούν σωστά. Προς τούτο ζητά την επανακκίνηση του υπολογιστή. Όταν την αποδεχτούμε, πριν φορτώσει το λειτουργικό θα κληθούμε να πληκτρολογήσουμε τον κωδικό που ορίσαμε προηγουμένως. Μια και δεν έχει ακόμα γίνει η κρυπτογράφηση, αν θέλουμε, μπορούμε να πατήσουμε το πλήκτρο [Esc] και να μην τον δώσουμε.



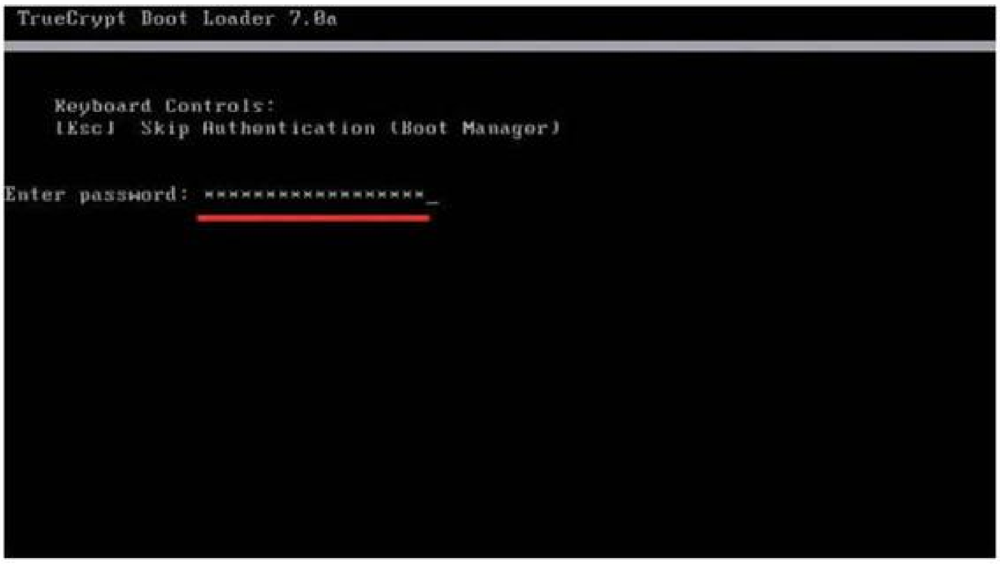


TrueCrypt Volume Creation Wizard
TRUECRYPT
Pretest Completed
The pretest has been successfully completed.
WARNING: Please note that if power supply is suddenly interrupted while encrypting existing data in place, or when the operating system crashes due to a software error or hardware malfunction while TrueCrypt is encrypting existing data in place, portions of the data will be corrupted or lost. Therefore, before you start encrypting, please make sure that you have backup copies of the files you want to encrypt. If you do not, please back up the files now (you can click Defer, back up the files, then run TrueCrypt again anytime, and select 'System' > 'Resume Interrupted Process' to start encrypting).
When ready, click Encrypt to start encrypting.
Help
< Back
Encrypt
Defer

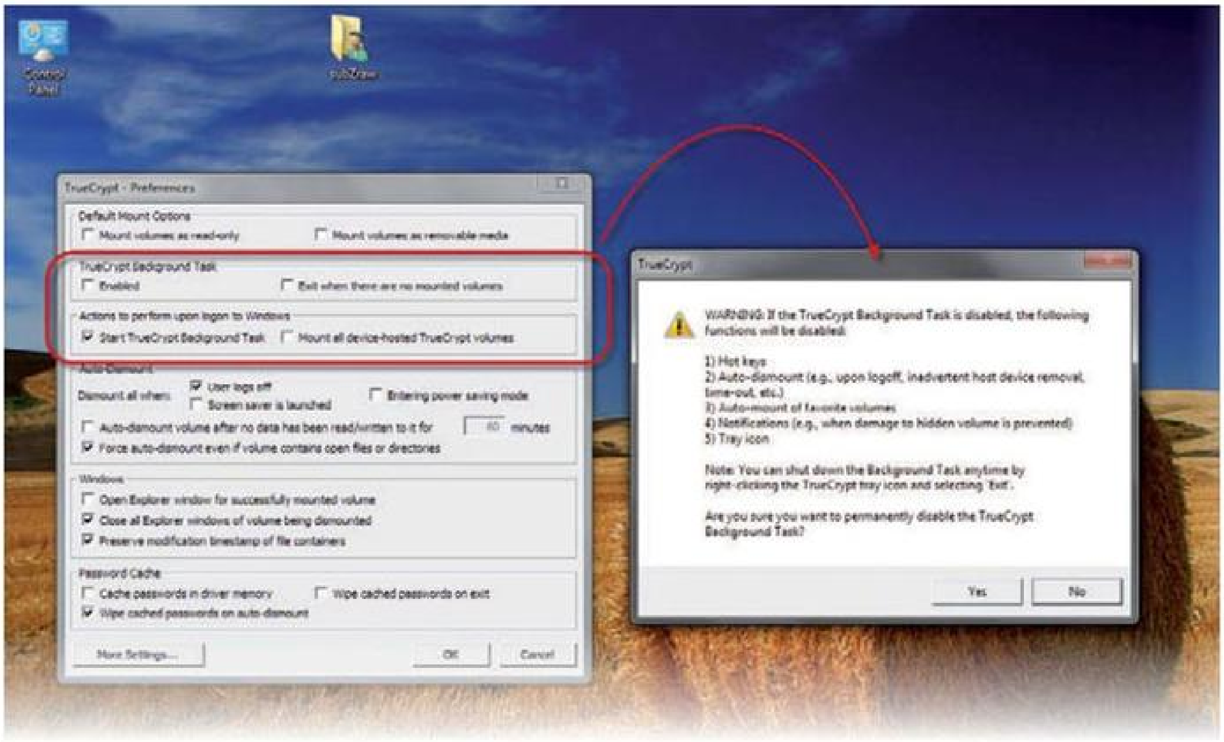

TrueCrypt Volume Creation Wizard
Pretest Completed
The pretest has been successfully completed.
User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: TrueCrypt
Verified publisher: TrueCrypt Foundation
File origin: Hard drive on this computer
Show details
Yes
No
Encrypt
Defer


TrueCrypt Volume Creation Wizard
TRUECRYPT
Encryption
Options
Wipe mode: None (fastest)
Pause
Done 76.079% Status Encrypting Left 12 minutes
You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, TrueCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.
More information
Help
< Back
Encrypt
Defer

Μετά τον επιτυχή, πρώτο έλεγχο, το TrueCrypt είναι έτοιμο να κρυπτογραφήσει το δίσκο ή το διαμέρισμα συστήματος. Φυσικά, το παράθυρο UAC των Windows θα παρεμβληθεί ζητώντας την επιβεβαίωσή μας. Ο χρόνος ολοκλήρωσης της διαδικασίας θα εξαρτηθεί κυρίως από μέγεθος του διαμερίσματος/δίσκου συστήματος. Σημειώστε ότι ανά πάσα στιγμή μπορούμε να σταματήσουμε τη διαδικασία και να τη συνεχίσουμε αργότερα από το ίδιο σημείο.



Μετά την κρυπτογράφηση του διαμερίσματος/δίσκου συστήματος, κάθε φορά που θ' ανοίγουμε το Windows PC/laptop μας θα πρέπει να πληκτρολογούμε τον κωδικό αποκρυπτογράφησης, διαφορετικά το λειτουργικό δεν θα μπορεί να ξεκινήσει.



Αν θέλατε το TrueCrypt μόνο για την κτυπρογράφηση του δίσκου/διαμερίσματος συστήματος, τότε δεν υπάρχει κανένας λόγος να τρέχει στο backgroud. Σημειώστε εδώ ότι *δεν* μπορείτε να το απεγκαταστήσετε πριν αποκρυπτογραφήσετε το δίσκο ή το διαμέρισμα συστήματος.

subZraw

Επιθέσεις ναι, μόνο από το Linux όχι!

Ό,τι και αν πείτε, δίκιο θα 'χετε. Καλό το Linux, δεν διαφωνούμε, αλλά σας έχουμε πρήξει πια μ' αυτό! Χάθηκαν δηλαδή τ' άλλα λειτουργικά συστήματα που χρησιμοποιεί ο κοσμάκης; Όχι βέβαια, καθόλου δεν χάθηκαν. Αυτός ο «κοσμάκης» μάλιστα τα χρησιμοποιεί για οποιαδήποτε δουλειά μπορείτε να φανταστείτε. Ναι, ακόμη και για penetration testing.

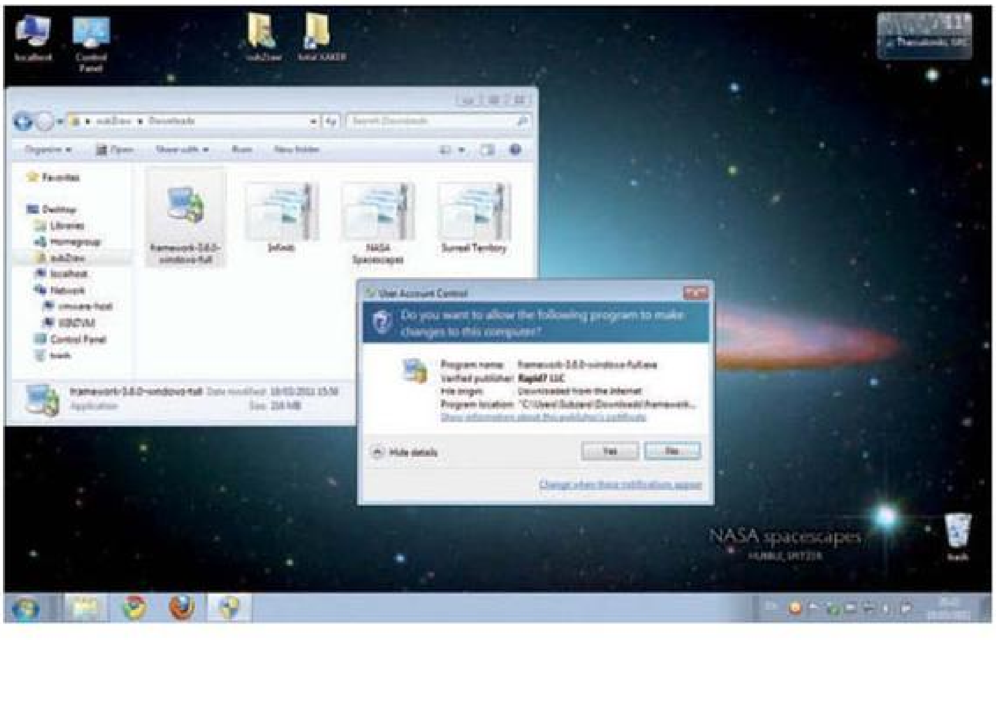
ΠΡΑΓΜΑΤΙ, κάπως έτσι φαίνεται να 'χουν τα πράγματα. Υπάρχουν λέει pen-testers που τρέχουν, π.χ., το Metasploit και το Armitage κάτω από τα Windows ή το Mac OS X. Προσέξτε: Δεν εννοούμε ότι σηκώνουν κάποιο virtual machine με BackTrack και μετά δουλεύουν μέσα απ' αυτό. Εννοούμε ότι τρέχουν το Metasploit και το Armitage *απευθείας* κάτω από Windows ή Mac OS X. Πέρα από το τι θα μπορούσε να σκεφτεί ή να σχολιάσει κάποιος γι' αυτές τις πρακτικές, η αλήθεια είναι ότι έπειτα από μια σύντομη αναζήτηση στο Google διαπιστώνουμε ότι υπάρχουν αρκετοί οδηγοί για την εγκατάσταση των Metasploit και Armitage στα δύο προαναφερθέντα λειτουργικά συστήματα. Φαίνεται μάλιστα ότι η διαδικασία είναι σαφώς ευκολότερη όταν έχουμε να κάνουμε με τα Windows, παρά με το Mac OS X.
Η όλη ιδέα είναι σίγουρα ενδιαφέρουσα – και πιστεύουμε ότι δεν χρειάζεται να 'ναι κανείς τρελά ανοιχτόμυαλος για να συμφωνήσει. Με δεδομένο αυτό, αλλά κι επειδή συχνά πυκνά η απόσταση μεταξύ θεωρίας και πράξης είναι τεράστια, είπαμε κι εμείς να εγκαταστήσουμε τα Metasploit και Armitage πρώτα κάτω από Windows και έπειτα κάτω από Mac OS X. Το παρόν άρθρο, λοιπόν, περιλαμβάνει δύο οδηγούς εγκατάστασης. Σ' αυτούς περιγράφουμε τα βήματα που εμείς ακολουθήσαμε, παραθέτοντας κι ορισμένες χρήσιμες, όπως θέλουμε να πιστεύουμε, επεξηγήσεις κι επισημάνσεις.

ΕΓΚΑΤΑΣΤΑΣΗ METASPLOIT ΚΑΤΩ ΑΠΟ WINDOWS

Η διαδικασία είναι η τυπική που συναντάμε στις εγκαταστάσεις προγραμμάτων κάτω από Windows, ωστόσο υπάρχουν ορισμένα σημεία τα οποία οφείλουμε να προσέξουμε. Αρχικά, πηγαίνετε μια βόλτα από το

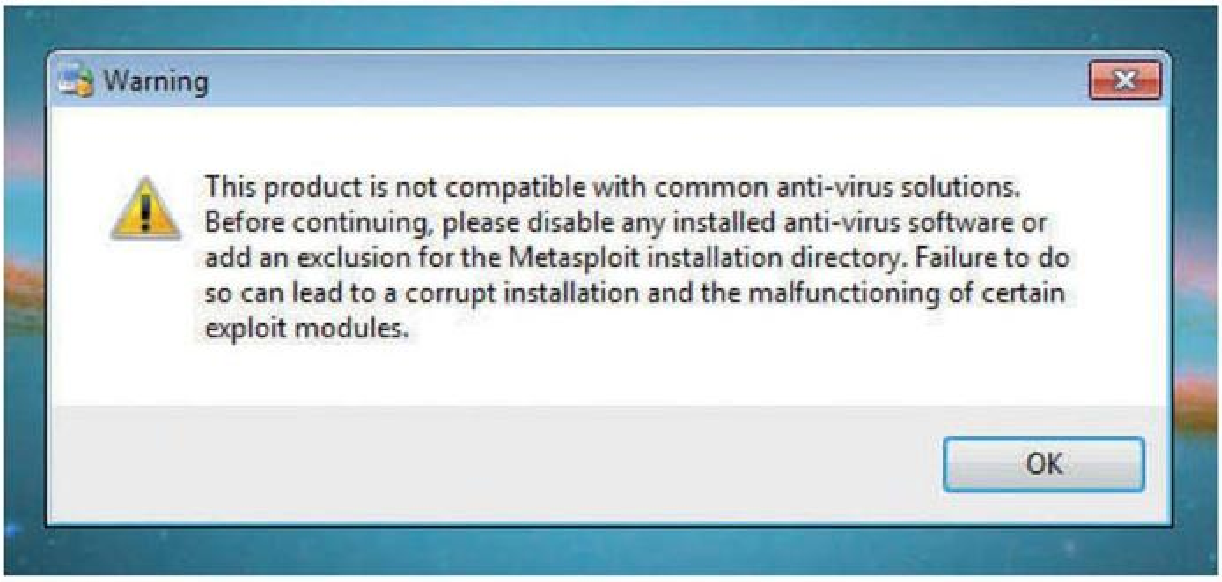
`www.metasploit.com/framework/download`

και κατεβάστε το αρχείο framework-3.6.0-windows-full.exe. Όταν ολοκληρωθεί η

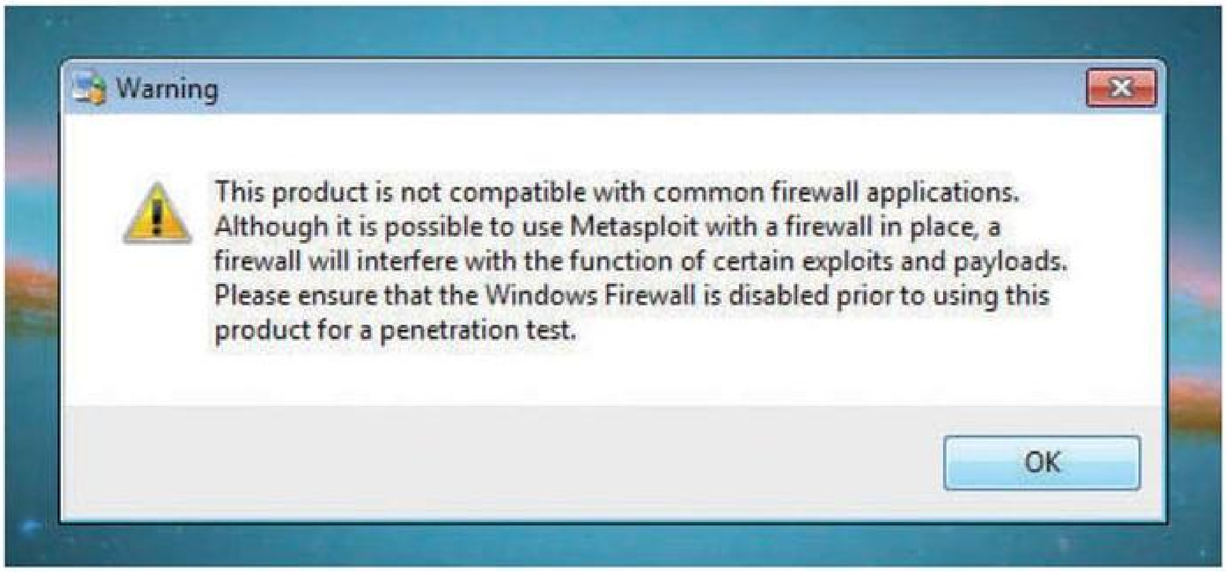


Ο installer του Metasploit πρέπει να τρέξει με δικαιώματα administrator, εξ ου και το παράθυρο του UAC.

λήψη, τρέξτε τον installer. Στα screenshots που ακολουθούν φαίνονται τα κυριότερα στάδια της εγκατάστασης.

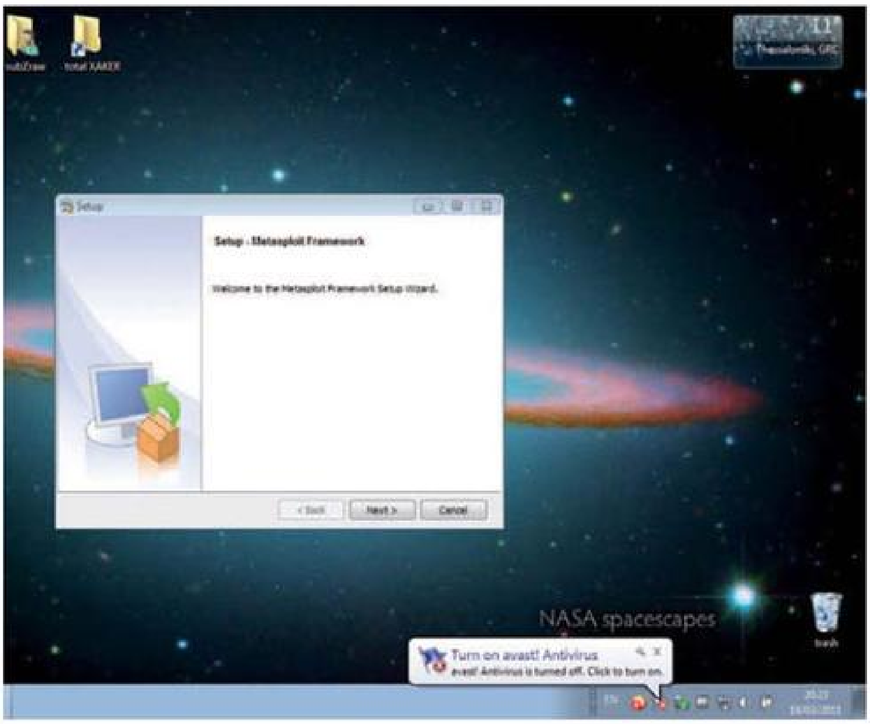


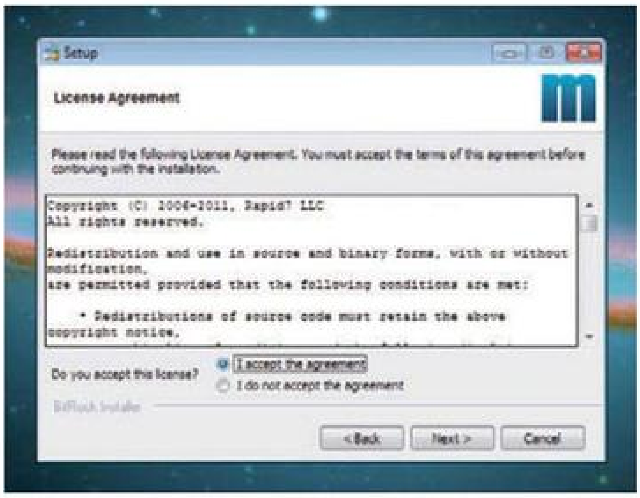
Πρώτη σημαντική σημείωση. Σχεδόν κάθε antivirus στον πλανήτη θα δημιουργήσει προβλήματα τόσο στην εγκατάσταση όσο και στη μετέπειτα χρήση του Metasploit κάτω από Windows. Προτείνεται, λοιπόν, κατά τη διάρκεια της εγκατάστασης ν' απενεργοποιήσετε το όποιο antivirus τρέχει στο σύστημα. Όταν η εγκατάσταση ολοκληρωθεί, θα μπορέσετε είτε να δημιουργήσετε μια εξαίρεση για το φάκελο εγκατάστασης του Metasploit (π.χ., c:\ program files\rapid7\framework) είτε ν' απενεργοποιείτε το antivirus πριν τρέχετε το Metasploit.

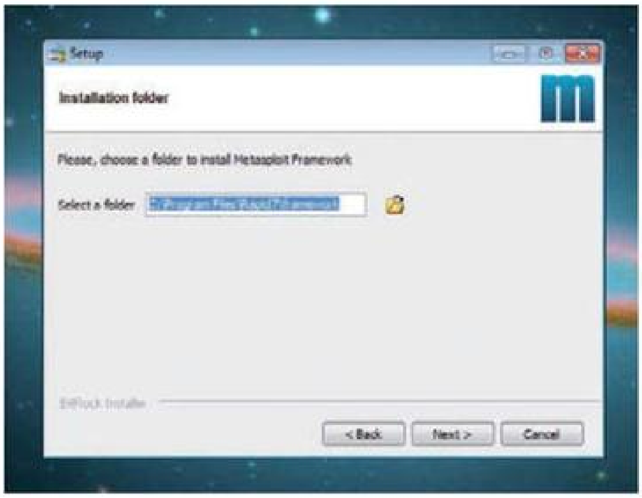


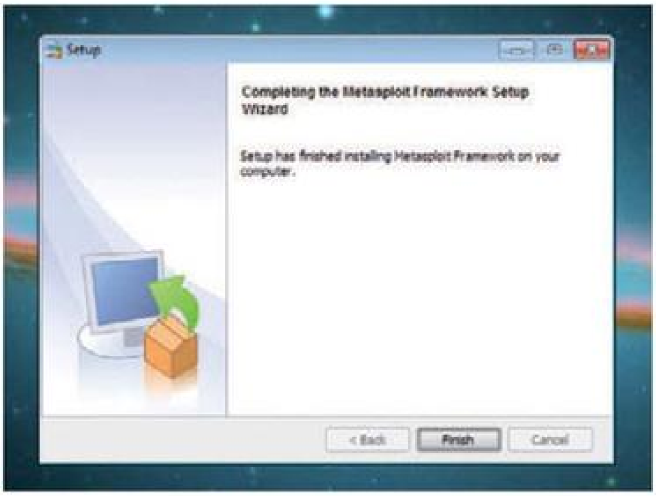
Δεύτερη σημαντική σημείωση. Αν και δεν χρειάζεται ν' απενεργοποιήσετε το firewall στο στάδιο της εγκατάστασης, αργότερα, κατά τη διάρκεια ενός pen-test, είναι τρομερά πιθανό να σας δημιουργήσει προβλήματα. Είτε, λοιπόν, θα δημιουργήσετε τους κατάλληλους κανόνες (εξαιρέσεις) είτε θα το απενεργοποιείτε προσωρινά. Σημειώστε ότι το firewall ενδέχεται να προκαλέσει προβλήματα πριν καν αρχίσει το pen-testing, αφού, π.χ., είναι πιθανό να εμποδίζει το Armitage να συνδέεται με τον RPC daemon του Metasploit.

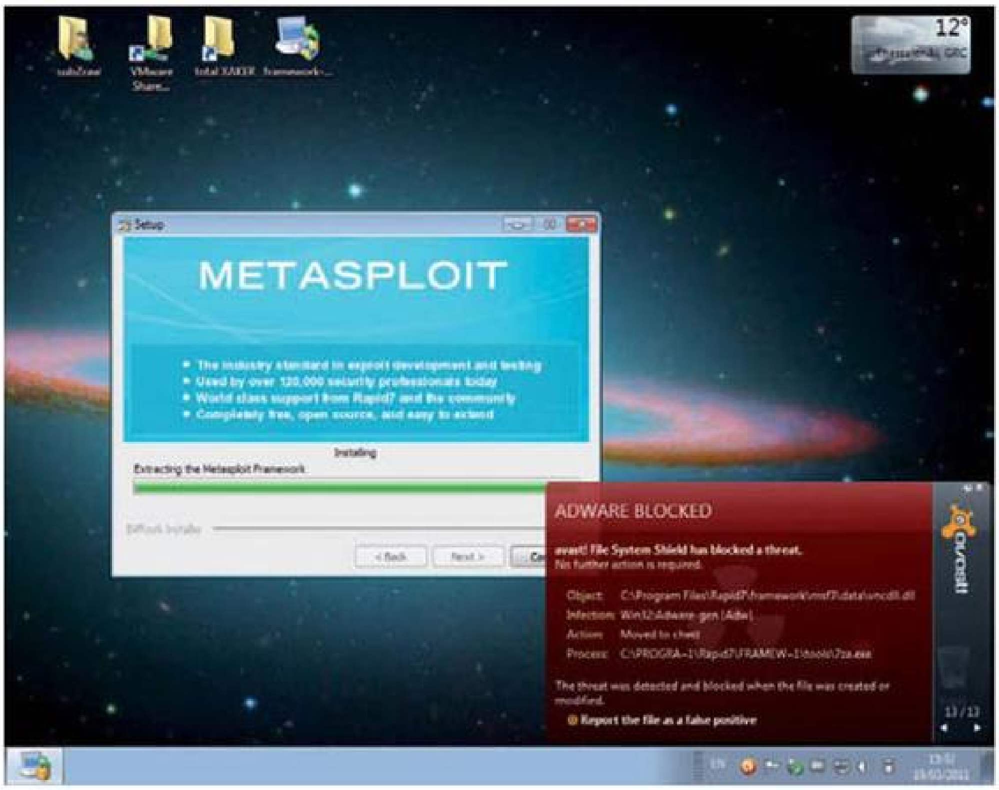
Αφού συμφωνήσουμε με την άδεια χρήσης και για το φάκελο εγκατάστασης, η διαδικασία ξεκινά, εξελίσσεται κι ολοκληρώνεται ομαλά. Προς το τέλος της θα αργήσει λίγο περισσότερο από το αναμενόμενο, όμως αυτό είναι φυσιολογικό. (Δεν ξέρουμε αν μας φαντασθήκατε, αλλά μόλις κάναμε air-quotes.)





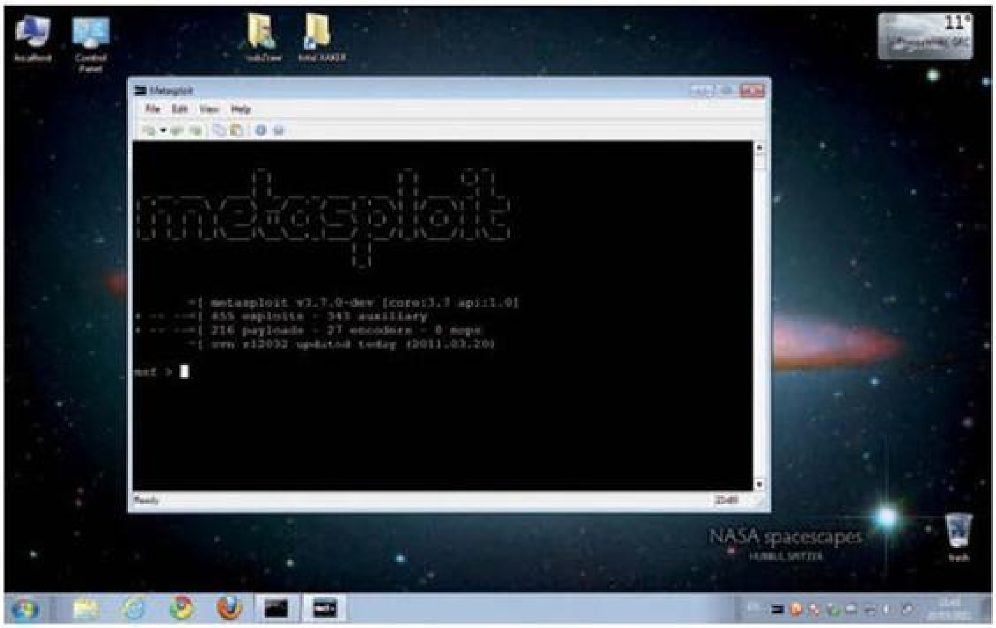




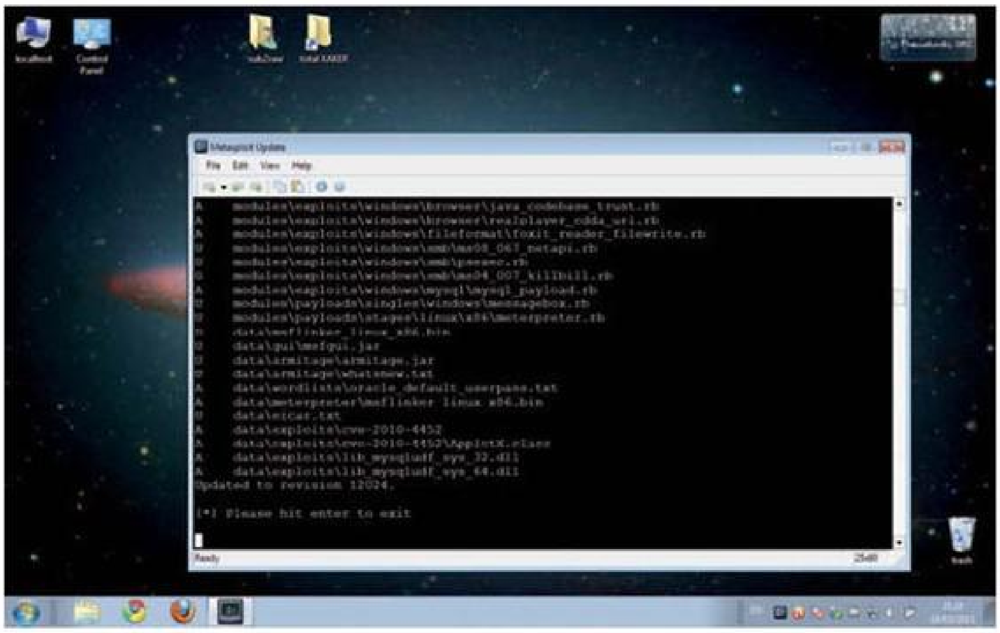


Με το antivirus ενεργοποιημένο το πιθανότερο είναι ότι δεν θα μπορέσετε καν να ολοκληρώσετε επιτυχώς την εγκατάσταση του Metasploit :S

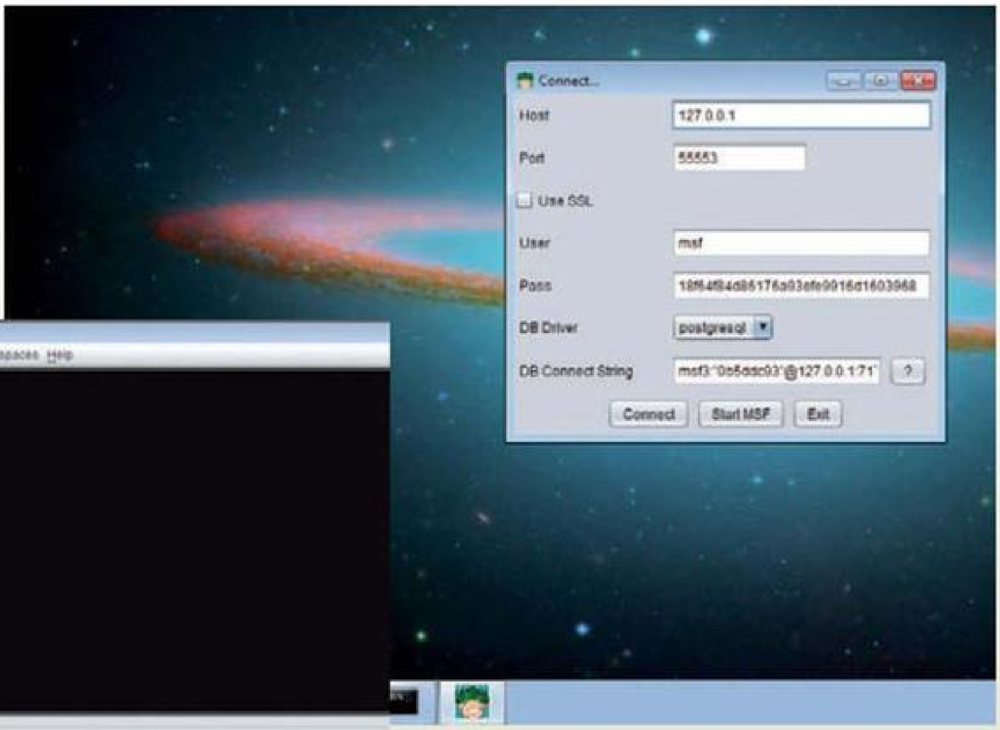
Μετά το πέρας της εγκατάστασης, στο μενού προγραμμάτων των Windows θα υπάρχει ένας φάκελος με όνομα Metasploit Framework. Μέσα σ' αυτόν βρίσκονται shortcuts προς διάφορα προγράμματα της πλατφόρμας, όπως εκείνο της αναβάθμισης (Metasploit Update), της κονσόλας (Metasploit Console) και του Armitage. Προτείνεται το καθένα απ' αυτά να το τρέχετε με δικαιώματα administrator: Απλά κάντε δεξί κλικ πάνω στ' όνομά του κι επιλέξτε Run as administrator.

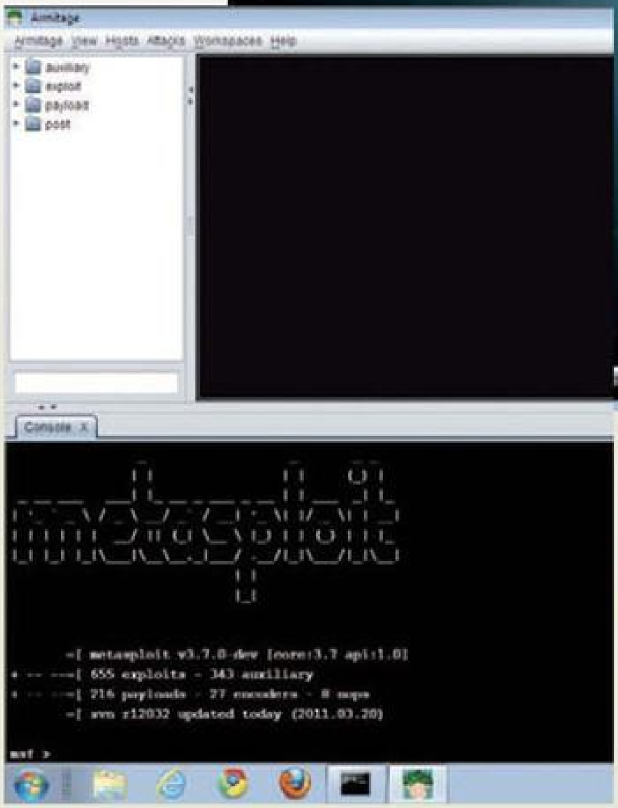


Ιδού η κλασική κονσόλα του Metasploit, μέσα από τα Windows. Τι άλλο θα δουν τα ματάκια μας, δηλαδή :)

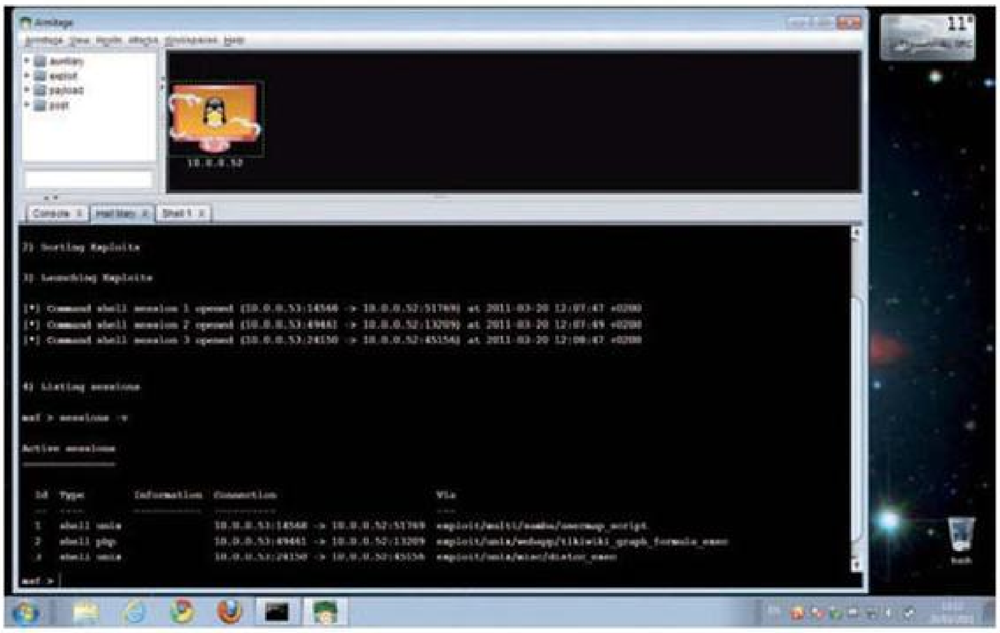


Η διαδικασία αναβάθμισης της τοπικής εγκατάστασης του Metasploit μ' όλα τα τελαυταία exploits μόλις ολοκληρώθηκε – κι ολοκληρώθηκε επιτυχώς.





Οι πρόσφατες εκδόσεις του Metasploit περιλαμβάνουν και το Armitage. Για να το τρέξετε πηγαίνετε στο μενού των Windows και συγκεκριμένα στο φάκελο Metasploit Framework, κάντε δεξί κλικ πάνω στην καταχώριση Armitage κι από το αναδυόμενο μενού διαλέξτε το Run as administrator. Στο παραθυράκι που θα εμφανιστεί πατήστε απλά το κουμπί Start MSF και περιμένετε. Έπειτα από λίγα δευτερόλεπτα θα δείτε το γνώριμο περιβάλλον του Armitage. Αν δεν σας είναι γνώριμο, μην ανησυχείτε: Φταίει που δεν έχετε ακόμη διαβάσει τα σχετικά άρθρα στα τεύχη 40 και 41 του total XAKER :D



Επίθεση σε σύστημα Linux μέσα από σύστημα Windows: Τα πάνω κάτω ή ο λειτουργικός αγνωστικισμός του καλού χάκερ στην πράξη; :D

ΕΓΚΑΤΑΣΤΑΣΗ METASPLOIT ΚΑΤΩ ΑΠΟ MAC OS X

Εδώ η διαδικασία είναι περισσότερο μακροσκελής, παραμένει όμως εύκολη. Ας τη δούμε αναλυτικά. (Όπως πάντα, με κίτρινο χρώμα είναι τονισμένο το input του χρήστη.)

Βήμα 1, εγκατάσταση MacPorts. Το εν λόγω σύστημα διαχείρισης εφαρμογών Unix για το Mac OS X το είχαμε παρουσιάσει εκτενώς στο τεύχος 32. Το σχετικό άρθρο το έχουμε αναδημοσιευμένο online στο Επίσημο Ανεπίσημο bl0g του περιοδικού. Μπορείτε να το διαβάσετε στη σελίδα

`http://txaker.defiant.gr/?p=3690`

Αν, λοιπόν, χρειάζεται, εγκαταστήστε το MacPorts και μάθετε τα βασικά για τη χρήση του. Πριν συνεχίσουμε. φροντίστε ώστε το τοπικό ports tree να 'ναι ενημερωμένο: Ανοίξτε ένα παράθυρο τερματικού και πληκτρολογήστε

```
mblack:~ cvar$ sudo port selfupdate
Password:
--->  Updating the ports tree
--->  Updating MacPorts base sources using rsync
MacPorts base version 1.9.2 installed,
MacPorts base version 1.9.2 downloaded.
--->  MacPorts base is already the latest version

The ports tree has been updated. To upgrade your installed ports,
you should run
  port upgrade outdated
```

Μην κλείσετε το τερματικό, θα το χρειαστούμε για τη συνέχεια.
Προσοχή! Στη μεταβλητή περιβάλλοντος PATH ο κατάλογος /opt/local/bin θα πρέπει να 'χει προτεραιότητα έναντι του /usr/bin, όπως στο παράδειγμα:

```
mblack:~ cvar$ echo $PATH
/opt/local/bin:/opt/local/sbin:/usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin:/usr/X11/bin:/Library/Application Support/VMware Fusion/
```

Αν χρειαστεί ν' αλλάξετε τη μεταβλητή PATH στο Mac OS σας κι έχετε ήδη διαβάσει το άρθρο μας από την προαναφερθείσα διεύθυνση του Επίσημου Ανεπίσημου bl0g, τότε ξέρετε πώς να το πετύχετε :)

Βήμα 2, εγκατάσταση Ruby. Πρόκειται για την αντικειμενοστρεφή σκριπτογλώσσα στην οποία είναι γραμμένο το Metasploit. Με τη βοήθεια του MacPorts εγκαθιστούμε την έκδοση 1.9 της γλώσσας:

```
mblack:~ cvar$ sudo port install ruby19 +nosuffix
--->  Computing dependencies for ruby19
--->  Fetching ruby19
--->  Verifying checksum(s) for ruby19
--->  Extracting ruby19
--->  Configuring ruby19
--->  Building ruby19
--->  Staging ruby19 into destroot
--->  Installing ruby19 @1.9.2-p180_0+nosuffix
--->  Activating ruby19 @1.9.2-p180_0+nosuffix
--->  Cleaning ruby19
```

Την οδηγία +nosuffix τη δώσαμε επειδή δεν θέλουμε να μπει το επίθεμα «19» στα εκτελέσιμα της Ruby. Έχετε υπόψη ότι μια διαφορετική έκδοση της Ruby ήταν ήδη εγκατεστημένη στο Mac OS X, πριν βάλουμε την 1.9. Το εκτελέσιμο του διερμηνευτή της άλλης έκδοσης κατοικεί στον κατάλογο /usr/bin. Χάρη όμως στη μεταβλητή περιβάλλοντος $PATH, η οποία δίνει προτεραιότητα στον κατάλογο /opt/local/bin όπου πηγαίνουν τα εκτελέσιμα του MacPorts, στο εξής όποτε τρέχουμε το διερμηνευτή της Ruby θα ενεργοποιείται εκείνος της έκδοσης 1.9:

```
mblack:~ cvar$ which ruby
/opt/local/bin/ruby
```

Πάρα πολύ ωραία.

Βήμα 3, εγκατάσταση της PostgreSQL. Για κάποιες λειτουργίες το Metasploit χρειάζεται μια βάση δεδομένων και η PostgreSQL είναι η προτιμώμενη.

Εγκαθιστούμε ως ακολούθως:

```
mblack:~ cvar$ sudo port install postgresql84-server
--->  Computing dependencies for postgresql84-server
...
--->  Activating postgresql84-server @8.4.7_0
--->  Cleaning postgresql84-server

mblack:~ cvar$ export PATH=/opt/local/lib/postgresql84/
bin/:"$PATH"
mblack:~ cvar$ sudo gem install pg
Building native extensions.  This could take a while...
Successfully installed pg-0.10.1
1 gem installed
Installing ri documentation for pg-0.10.1...
Installing RDoc documentation for pg-0.10.1...
```

Χάρη στις δύο τελευταίες εντολές εγκαταστήσαμε και τη βιβλιοθήλη της Ruby ονόματι pg, ώστε μέσα από τη γλώσσα να 'ναι δυνατή η επικοινωνία με τις βάσεις δεδομένων της PostgreSQL.

Βήμα 4, λήψη κι εγκατάσταση Metasploit. Φτιάχνουμε ένα βολικό κατάλογο για το Metasploit:

```
mblack:~ cvar$ sudo mkdir /opt/metasploit3
```

Με χρήση ενός εργαλείου σαν το wget, το οποίο, αν δεν το 'χετε ήδη, μπορείτε να το εγκαταστήσετε από το MacPorts, κατεβάζουμε στο Mac μας την τελευταία έκδοση του Metasploit (τη στιγμή που γράφονται αυτές οι γραμμές η πλέον πρόσφατη έκδοση είναι η 3.6.0 και το αρχείο που θέλουμε είναι το framework-3.6.0.tar.bz2):

```
mblack:~ cvar$ cd /opt/metasploit3
mblack:metasploit3 cvar$ sudo wget http://updates.metasploit.com/
data/releases/framework-3.6.0.tar.bz2
-2011-03-19 18:27:13--  http://updates.metasploit.com/data/releas-
es/framework-3.6.0.tar.bz2
Resolving updates.metasploit.com (updates.metasploit.com)...
184.154.104.2
Connecting to updates.metasploit.com (updates.metasploit.
com)|184.154.104.2|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 47125266 (45M) [application/x-bzip2]
```

```
Saving to: `framework-3.6.0.tar.bz2'

100%[======================================>] 47,125,266   148K/s
in 3m 57s

2011-03-19 18:31:11 (194 KB/s) - `framework-3.6.0.tar.bz2' saved
[47125266/47125266]
```

Εναλλακτικά, το Unix archive του Metasploit μπορείτε να το κατεβάσετε μ' έναν web browser από τη διεύθυνση

`www.metasploit.com/framework/download`

Μετά την ολοκλήρωση της λήψης αποσυμπιέζουμε – πάντα μέσα στον κατάλογο στον οποίο έχουμε επιλέξει να εγκαταστήσουμε το Metasploit:

```
mblack:metasploit3 cvar$ sudo tar jxf framework-3.6.0.tar.bz2 -o
```

Βήμα 5, αναβάθμιση κι ενεργοποίηση του Metasploit. Πηγαίνουμε στον κατάλογο όπου έχουμε εγκαταστήσει το Metasploit κι αναβαθμίζουμε:

```
mblack:msf3 cvar$ sudo ./msfupdate
[*]
[*] Attempting to update the Metasploit Framework...
[*]

U    test/functional/framework/msfconsole_spec.rb
U    test/functional/meterpreter/meterpreter_php_spec.rb
U    test/functional/meterpreter/meterpreter_java_spec.rb
...
A    data/exploits/cve-2010-4452/AppletX.class
A    data/exploits/lib_mysqludf_sys_32.dll
A    data/exploits/lib_mysqludf_sys_64.dll
Updated to revision 12022.
```

Μια χαρά. Το Metasploit το εκτελούμε ως εξής:

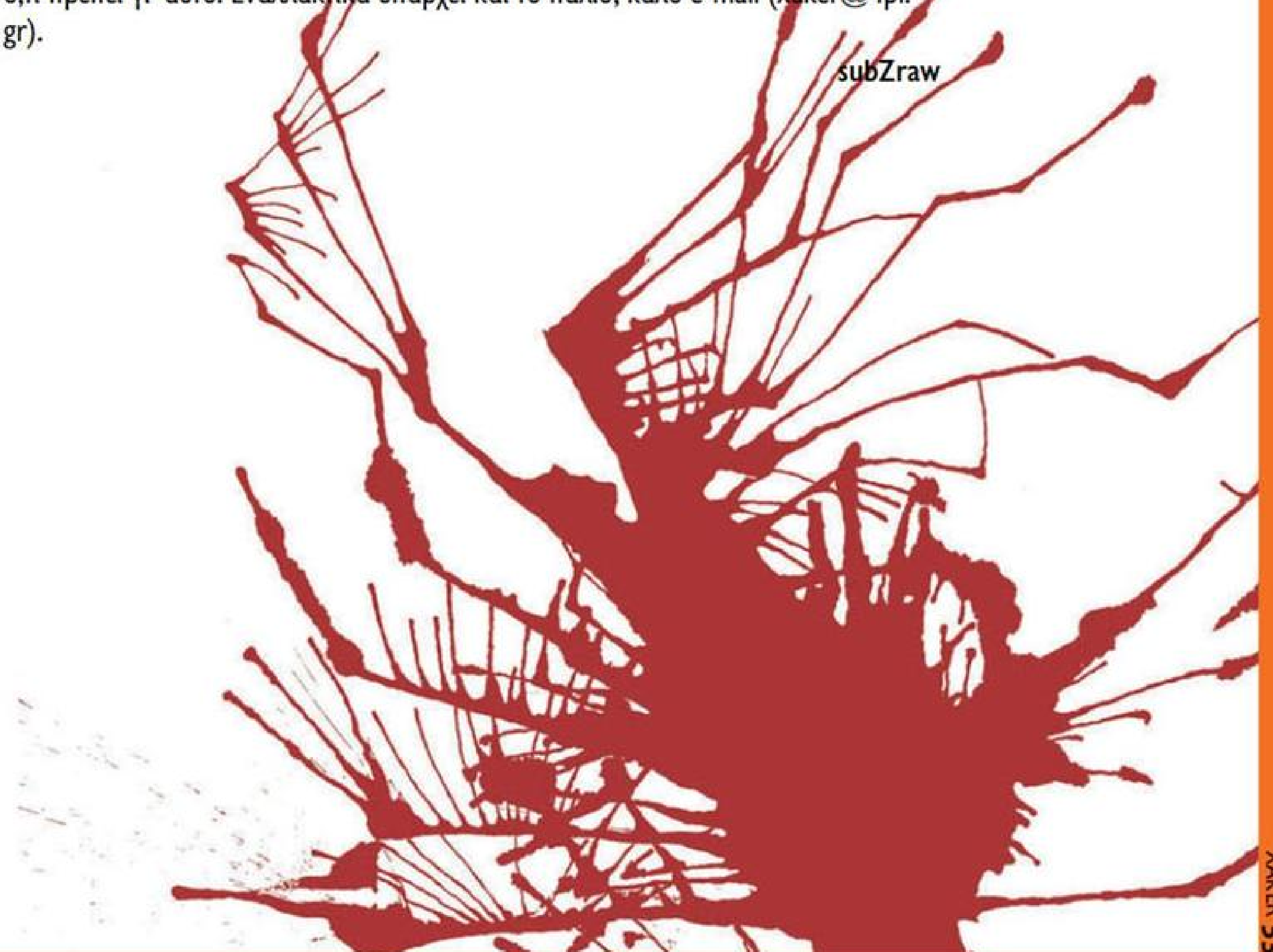
```
mblack:msf3 cvar$ sudo ./msfconsole
                _                  _       _ _
               | |                | |     (_) |
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___  _| |_
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __|
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | |_
```

```
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__|
                             | |
                             |_|


       =[ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- --=[ 655 exploits - 343 auxiliary
+ -- --=[ 216 payloads - 27 encoders - 8 nops
       =[ svn r12022 updated today (2011.03.18)

msf >
```

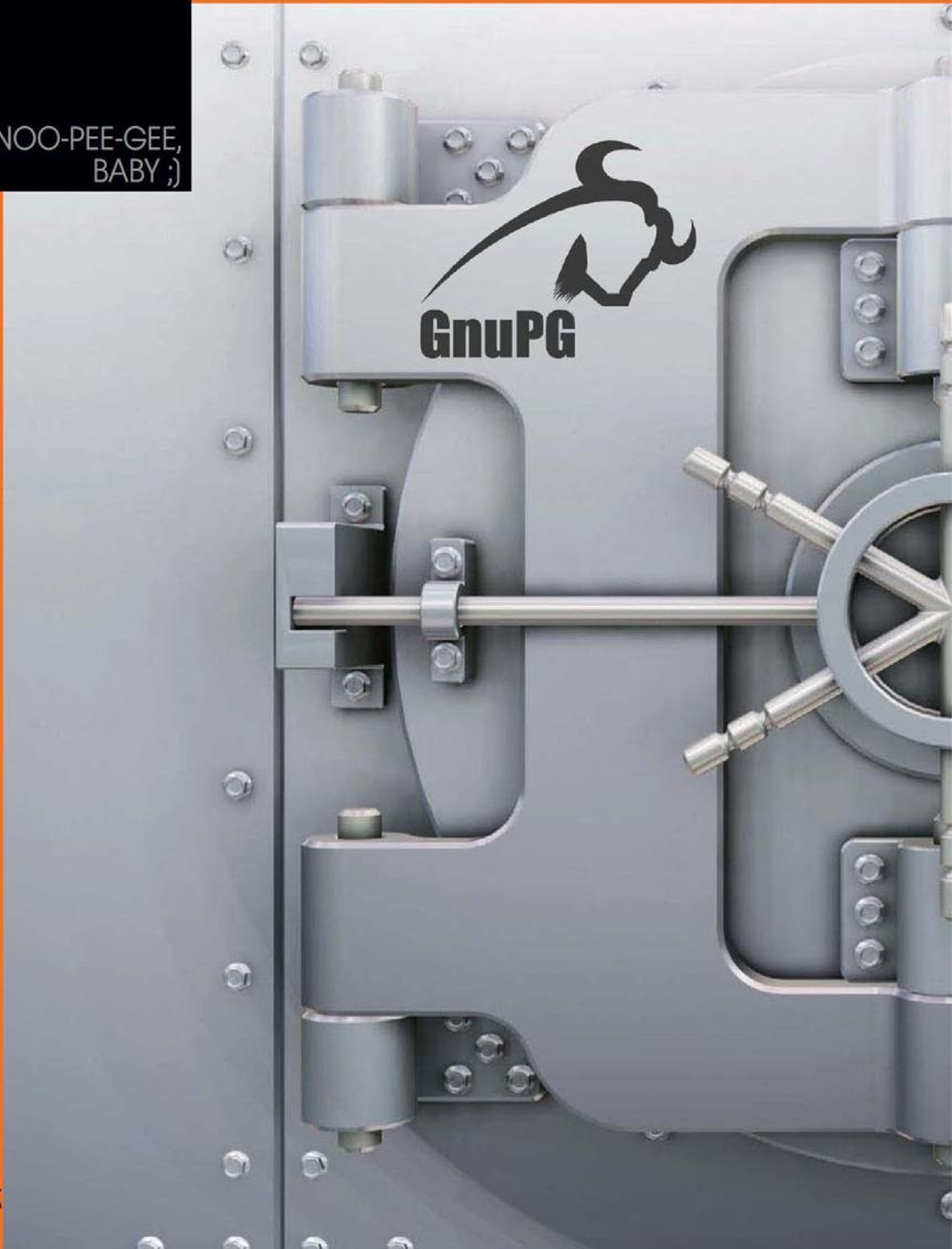
Προαιρετικά, την πλήρη διαδρομή της εγκατάστασης του Metasploit μπορούμε να την προσθέσουμε στη μεταβλητή περιβάλλοντος PATH, ώστε τα προγράμματα msfconsole, msfupdate, msfcli κ.λπ. να τα τρέχουμε ευκολότερα, σε όποιον κατάλογο κι αν βρισκόμαστε.

Σημείωση: Παρά τις προσπάθειές μας μέσα στα χρονικά περθώρια που διαθέταμε δεν καταφέραμε να τρέξουμε το Armitage επιτυχώς στο μηχάνημα της δοκιμής μας (Mac OS X 10.5.8). Όποιος τα καταφέρει θα θέλαμε να μας πει πώς ακριβώς το πέτυχε. Η fan page που έχουμε στο Facebook (www.facebook.com/totalxaker) είναι ό,τι πρέπει γι' αυτό. Εναλλακτικά υπάρχει και το παλιό, καλό e-mail (xaker@4pi.gr).

subZraw



GNOO-PEE-GEE, BABY ;)



Διάβασέ το, αν μπορείς!

Δεν έχει καμία σημασία πώς θα φτάσει το mail ή τα αρχεία σας από το σημείο Α στο σημείο Β. Μπορεί να πάει απευθείας, μπορεί να περάσει πρώτα από το Γ, μπορεί και μέσω όλων των γραμμάτων της αλφαβήτου. Σημασία έχει ότι κανείς δεν θα μπορέσει να τα υποκλέψει, όσο πονηρός ή/και ικανός κι αν είναι. Για την ακρίβεια –και για να μη λέμε ό,τι θέλουμε– δεν αποκλείεται να τα καταφέρει κι όντως να τα υποκλέψει. Ακόμα και τότε, όμως, θα του είναι εντελώς άχρηστα! Εκτός βέβαια κι αν *δεν* είχατε μεριμνήσει να χρησιμοποιήσετε το GnuPG.

ΚΑΤΙ ΜΑΣ ΛΕΕΙ ΟΜΩΣ ότι αποκλείεται να μη χρησιμοποιείτε το GnuPG, ειδικά μάλιστα αν μιλάμε για mail ή αρχεία που περιλαμβάνουν ευαίσθητες πληροφορίες ή δεδομένα. Το GnuPG είν' ένα πανίσχυρο σύστημα κρυπτογραφίας δημοσίου κλειδιού, το οποίο παρουσιάζουμε εκτενώς στο άρθρο που αρχίζει από τη σελίδα 6 του τεύχους που κρατάτε στα χέρια σας. Πέρα από τις απαραίτητες γνώσεις που πρέπει να 'χετε ώστε να το χρησιμοποιείτε αποτελεσματικά, στο ίδιο άρθρο παραθέτουμε κι αναλυτικά παραδείγματα για το πώς δημιουργούμε ζεύγη κλειδιών, πώς διανέμουμε τα δημόσια κλειδιά σ' όλους τους ενδιαφερόμενους, πώς ανακαλούμε κλειδιά που για οποιονδήποτε λόγο δεν ισχύουν κ.ο.κ. Στο παρόν άρθρο περνάμε σε πιο ενδιαφέροντα θέματα και δείχνουμε πώς χρησιμοποιούμε το GnuPG στην πράξη, για να κρυπτογραφούμε, να αποκρυπτογραφούμε, να υπογράφουμε και να ελέγχουμε υπογραφές. Όπως και στο άρθρο της σελίδας 6, δουλεύουμε κατά κύριο λόγο από τη γραμμή εντολών του openSUSE. Σε αντίθεση όμως με το άλλο άρθρο, σ' αυτό εδώ παρουσιάζουμε –εν συντομία– κι ορισμένα font-ends του GnuPG για το περιβάλλον γραφικών των Windows, του Mac OS X και φυσικά του Linux. Εννοείται πως από τη στιγμή που θα έχετε δουλέψει το GPG από τη γραμμή εντολών, δεν θα έχετε κανένα απολύτως πρόβλημα με την ορολογία και το interface οποιουδήποτε GUI.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΙ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ ΓΙΑ ΠΡΟΣΩΠΙΚΗ ΧΡΗΣΗ

Ας υποθέσουμε ότι θέλουμε να κρυπτογραφήσουμε ένα αρχείο, π.χ., το έγγραφο parabing.odt. Θα χρησιμοποιήσουμε το δημόσιο κλειδί μας κι επομένως κανείς άλλος δεν θα μπορεί να αποκρυπτογραφήσει το parabing.odt παρά εμείς οι ίδιοι, αφού μόνο εμείς διαθέτουμε το αντίστοιχο ιδιωτικό κλειδί. Ιδού πώς κρυπτογραφούμε:

```
sub  opensuse:~>  p  --armor --output parabin .odt. p  --recipient
sub raw --encr pt parabin .odt
```

Ακολουθεί η σημασία των παραμέτρων που περάσαμε στο gpg.

--armor:	Θέλουμε το κρυπτογραφημένο αρχείο να 'ναι σε μορφή ASCII
--outpout:	Δείχνουμε το αρχείο που θ' αποτελεί την κρυπτογραφημένη εκδοχή του πρωτότυπου αρχείου. Σε διαφορετική περίπτωση τα κρυπτογραφημένα δεδομένα πηγαίνουν στο standard output.
--recipient:	Ορίζουμε για ποιον προορίζεται η κρυπτογραφημένη μορφή, δίνοντας το όνομα χρήστη ή τη διεύθυνση mail που υπάρχει στο αντίστοιχο keypair
--encrypt:	Προφανής η σημασία της :)

Στο τέλος της εντολής μπαίνει το όνομα (ή η πλήρης διαδρομή) του αρχείου εισόδου, δηλαδή του πρωτότυπου αρχείου. Για να πραγματοποιηθεί η κρυπτογράφηση

θα πρέπει να πληκτρολογήσουμε και το passphrase του ιδιωτικού μας κλειδιού. Παρατηρήστε ότι το gpg αφήνει το πρωτότυπο αρχείο άθικτο κι απλά δημιουργεί ένα νέο, που είναι η κρυπτογραφημένη του εκδοχή:

```
sub  opensuse:~> ls -lh parabin .
-rw-r--r--   sub  users     ar     :   parabin .odt
-rw-r--r--   sub  users     ar     :   parabin .odt. p
```

Δείτε πώς μοιάζει το κρυπτογραφημένο αρχείο (δείχνουμε μόνο την αρχή και το τέλος του):

```
sub  opensuse:~> head parabin .odt. p
-----     P P    A -----
 ersion:  nuP  v . .      / inu

h   A ul  t haslA  A   AHh h   k  i  ns  i  /    T a/ a    o
 h hh  r  ht f  oif  TA  utb  k     hec       ewbdAlH     t  m /
T   e/v pi  c d  Pmc d   lm H b  A mc       f  b tfAne   P  mp w
5ejcQlViGQCjXniJkZ0l1/mH8FL17fSWwJRAW0br8Grp88CcLlGflJ+mTt7BUz+x
n  bmdkt    fe r       l c  m   Aw/ t    c  n /in       /    w r
  s oow   bm   m dA   hcr          h d nH  /AA   A    e/suvufvc
   nd      hp pTlnb m  pH A pb    t        Tuu l H   iab  v vbwH

sub  opensuse:~> tail parabin .odt. p
 r s    a  ws/t  H v kn      T          ss  / ub s saloT PeH u
     ci    t   n     wsu  re      f    r     P HApe un m h uph w
  w s  s  bo HP             s  n  iu i PT    rP    on  cm   H
  tn eH h      th t      e k  b  s a  T  v b r     d     c t
    H   kP pm    w   s  c f   uP Pb   d s  u iuP  /i l w w  bpd
 md A/  HHip aPca   T khu   a  l  Adb  ono     A  nhAnn tH ui r
ycHRk72IS57Ytrr8JfG2O3V9qynTny1yu5/uMkn1drVjy2bz1wDBofikWbP+zmX6
u d do  Ti /         c p wvA
    w
-----   P P    A -----
sub  opensuse:~>
```

Ωραιότατο! Παρακολουθήστε τώρα τι συμβαίνει όταν επιχειρεί να το αποκρυπτογραφήσει κάποιος που *δεν* έχει το ιδιωτικό μας κλειδί:

```
kun lao opensuse:~>  p  --output parabin .odt --decr pt parabin .
odt. p
 p : encr pted with     -bit  A ke       A  A    created     -
  -
```

```
      "subZraw (Underworld SA) <subZraw@defiant.gr>"
 p : decr ption failed:  o secret ke
kun lao opensuse:~>
```

Αρκετά σαφές το μήνυμα. Όταν όμως επιχειρήσουμε να το αποκρυπτογραφήσουμε εμείς, τότε όλα καλά:

```
sub  opensuse:~>  p  --output parabin .odt --decr pt parabin .odt.
 p

 ou need a passphrase to unlock the secret ke  for
user: "subZraw (Underworld SA) <subZraw@defiant.gr>"
    -bit   A ke       A  A     created     -  -    main ke
       A

 p : encr pted with     -bit   A ke       A  A     created    -
  -
      "subZraw (Underworld SA) <subZraw@defiant.gr>"
sub  opensuse:~>
```

Το μόνο που χρειάστηκε ήταν το passphrase, αλλά αυτό ήταν απολύτως αναμενόμενο. Πέρα από μεμονομένα αρχεία, το gpg μπορεί να κρυπτογραφεί πολλά αρχεία, με μιας. Γι' αυτή τη δουλειά χρειάζεται η παράμετρος --multifile. Ας πούμε, π.χ., ότι θέλουμε να κρυπτογραφήσουμε όλα τα αρχεία του καταλόγου ConfessionsOfAnEconomicHitman:

```
sub  opensuse:~> gpg --armor --recipient subZraw --multifile --en
cr pt  onfessions fAn conomicHitman/
```

Παρατηρήστε ότι δεν δώσαμε την παράμετρο --output. Μετά το πέρας της διαδικασίας, μέσα στον κατάλογο ConfessionsOfAnEconomicHitman για κάθε αρχείο θα υπάρχει και η κρυπτογραφημένη του εκδοχή, με ίδιο όνομα και την κατάληξη «.asc». Η παράμετρος --multifile χρησιμεύει κι όποτε θέλουμε ν' αποκρυπτογραφήσουμε πολλά αρχεία μαζί:

```
sub  opensuse:~> gpg --multifile --decrypt ConfessionsOfAnEco
nomicHitman/
 ou need a passphrase to unlock the secret ke  for
user: "subZraw (Underworld SA) <subZraw@defiant.gr>"
...
sub  opensuse:~>
```

ΚΡΥΠΤΟΓΡΑΦΗΣΗ/ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ ΓΙΑ ΑΠΟΣΤΟΛΗ/ΛΗΨΗ

Για να στείλουμε σε κάποιον ένα κρυπτογραφημένο αρχείο που θα μπορέσει να αποκρυπτογραφήσει, το κρυπτογραφούμε με χρήση του δημοσίου του κλειδιού. Ας πούμε, π.χ., ότι θέλουμε να στείλουμε στον Kung Lao το parabing.odt σε κρυπτογραφημένη μορφή. Αρχικά φροντίζουμε να πάρουμε το public key του Kung Lao και να το αποθηκεύσουμε στο αντίστοιχο keyring μας. Αυτό επιτυγχάνεται πολύ πιο εύκολα απ' όσο ακούγεται:

```
sub  opensuse:~> p  --search-ke  " un   ao"
 p : searchin  for " un   ao" from hkp server ke s. nup .net
        un   ao  elative of  iu  an    kun lao freemail. r>
              bit   A ke            created:     -  -
        un   ao  kun lao  abber.ccc.de>
              bit   A ke          A  created:     -  -
        un   ao  kun  lao  m .net>
              bit   A ke            created:     -  -
        un   ao  kun  lao  m .net>
              bit   A ke            created:     -  -
 e s  -  of   for " un   ao".  nter number s     e t  or   uit >
 p : re uestin  ke            from hkp server ke s. nup .net
 p : ke          : public ke  " un   ao   elative of  iu  an
 kun lao freemail. r>" imported
 p : Total number processed:
 p :               imported:       A:
sub  opensuse:~>
```

Βλέπουμε ότι υπάρχουν διάφοροι Kung Lao, ο δικός μας όμως ξέρουμε ότι έχει mail στο FreeMail, επομένως είναι προφανές ποιο κλειδί πρέπει να επιλέξουμε. Στη συνέχεια κρυπτογραφούμε όπως δείξαμε προηγουμένως, προσέχουμε όμως να περάσουμε στην παράμετρο --recipient το όνομα του παραλήπτη κι όχι το δικό μας:

```
sub  opensuse:~> p  --armor --output parabin  u.odt. p  --recipi
ent " un   ao" --encr pt parabin .odt
 p :  AA     : There is no assurance this ke  belon s to the named
user

pub       / AA           -  -    un   ao   elative of  iu  an
 kun lao freemail. r>
 Primary key fingerprint: 0B41 4973 4038 A040 A21B  F56A CC17 2514

      Subkey fingerprint: D16D ADD8 37F1 EA16 67DB  AF86 9919 EA62
 AA
```

```
 t is   T certain that the ke  belon s to the person named
in the user   .   f  ou  reall   know what  ou are doin
 ou ma  answer the ne t  uestion with  es.

 se this ke  an wa     /
sub  opensuse:~>
```

Το gpg γκρίνιαξε λίγο, θυμίζοντάς μας ότι δεν υπάρχει καμιά εγγύηση ότι το δημόσιο κλειδί με το οποίο πάμε να κρυπτογραφήσουμε ανήκει πράγματι στον άνθρωπο που νομίζουμε ότι ανήκει. Εμείς όμως ξέρουμε τι κάνουμε γι' αυτό και του λέμε να συνεχίσει. Εκείνο σηκώνει τα χέρια ψηλά ξεφυσώντας και προχωρά. (Ανά πάσα στιγμή έχουμε τη δυνατότητα να υπογράψουμε το δημόσιο κλειδί του Kung Lao, με τον τρόπο που δείξαμε στο άρθρο της σελίδας 6. Αφού το κάνουμε, το gpg δεν θα παραπονιέται κάθε φορά που θα πηγαίνουμε να κρυπτογραφήσουμε με το δημόσιο κλειδί του Kung Lao.) Είμαστε τώρα έτοιμοι να στείλουμε το αρχείο parabing4u.odt.gpg στον Kung Lao, π.χ., ως attachment σε mail. Όταν εκείνος το λάβει δεν θα 'χει κανένα πρόβλημα να το αποκρυπτογραφήσει:

```
kun lao opensuse:~>  p  --output parabin  me.odt --decr pt para
bin  u.odt. p

 ou need a passphrase to unlock the secret ke  for
user: " un   ao   elative of  iu  an    kun lao freemail. r>"
    -bit   A ke       AA       created      -  -    main ke


 p : encr pted with      -bit   A ke       AA       created     -
  -
      " un   ao   elative of  iu  an    kun lao freemail. r>"

kun lao opensuse:~> ls -lh parabin
-rw-r--r--   kun lao users      ar       :   parabin  me.odt
-rw-r--r--   kun lao users      ar       :   parabin  u.odt. p
kun lao opensuse:~>
```

Το μόνο που χρειάστηκε να δώσει ο φίλος μας ήταν το passphrase του.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ/ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ MAIL

Για το ίδιο το περιεχόμενο ενός mail εργαζόμαστε παρόμοια με την περίπτωση κρυπτογράφησης/αποκρυπτογράφησης αρχείων. Αναλυτικότερα, ετοιμάζουμε ένα έγγραφο με το περιεχόμενο, το κρυπτογραφούμε με το δημόσιο κλειδί του παραλήπτη και κατόπιν του στέλνουμε ένα mail με το κρυπτογραφημένο έγγραφο ως συνημμένο. Εκείνος ανοίγει το mail, αποθηκεύει το συνημμένο έγγραφο στον

υπολογιστή του κι ακολούθως το αποκρυπτογραφεί με χρήση του ιδιωτικού του κλειδιού. Υπάρχουν mail clients, όπως το Kmail και το Evolution, οι οποίοι υποστηρίζουν αυτόματη κρυπτογράφηση/αποκρυπτογράφηση/υπογραφή των διακινούμενων mail. Αντί δηλαδή να κρυπτογραφούμε ξεχωριστά το περιεχόμενο και να το στέλνουμε ως συνημμένο, συντάσσουμε κανονικά το mail, πριν την αποστολή επιλέγουμε να το κρυπτογραφήσουμε ή/και να το υπογράψουμε κι ακολούθως το στέλνουμε. Αν ο παραλήπτης έχει mail client με ανάλογες δυνατότητες, το κρυπτογραφημένο mail το διαβάζει μ' ένα μόλις κλικ – άντε και με την εισαγωγή του passphrase που προστατεύει το ιδιωτικό του κλειδί.

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Όποτε θέλουμε να στείλουμε ένα αρχείο ή κάποιο mail και να βεβαιώνουμε τους παραλήπτες για την πραγματική μας ταυτότητα, τότε οφείλουμε να το υπογράφουμε. Ουσιαστικά, η υπογραφή είν' ένα string που κρυπτογραφείται με χρήση του *ιδιωτικού* μας κλειδιού και επισυνάπτεται στο αρχείο ή στο mail. Ο ενδιαφερόμενος παραλήπτης είναι σε θέση να δοκιμάσει την αποκρυπτογράφηση της υπογραφής με χρήση του δημοσίου μας κλειδιού. Αν τα καταφέρει τότε μπορεί να 'ναι βέβαιος ότι, πράγματι, το αρχείο ή το mail έχει προέλθει από εμάς, αφού μόνο εμείς έχουμε πρόσβαση στο αντίστοιχο ιδιωτικό κλειδί!

Έχουμε την επιλογή να υπογράφουμε αρχεία ή mail, ανεξαρτήτως αν τα κρυπτογραφούμε κιόλας ή όχι. Ας δούμε πρώτα ένα παράδειγμα υπογραφής αρχείου *χωρίς* κρυπτογράφηση.

```
sub  opensuse:~>  p  --si n --detach-si n parabin .odt

 ou need a passphrase to unlock the secret ke  for
user: "subZraw (Underworld SA) <subZraw@defiant.gr>"
    -bit   A ke             A  created    -  -

sub  opensuse:~> ls -lh parabin .odt
-rw-r--r--   sub  users      ar      :   parabin .odt
-rw-r--r--   sub  users      ar      :   parabin .odt.si
sub  opensuse:~>
```

Την παράμετρο --detach-sign τη βάλαμε επειδή θέλαμε την υπογραφή του αρχείου parabing.odt σε ξεχωριστό αρχείο κι όχι ένα νέο αρχείο με επικολλημένη την υπογραφή. Αν τώρα στείλουμε σ' έναν χρήστη –ο οποίος έχει το δημόσιο κλειδί μας– τα αρχεία parabing.odt και parabing.odt.sig, τότε εκείνος θα μπορεί να επαληθεύσει ότι τα έλαβε από εμάς:

```
kun lao opensuse:~>  p  parabin .odt.si
 p :  i nature made  ed      ar          :  :   P     T usin     A ke
```

```
        A
gpg: Good signature from "subZraw (Underworld SA) <subZraw@defiant.
 r>"
 p :                 aka "sub raw  This ain t  im  eam   sub raw
parabin .com>"
gpg: WARNING: This key is not certified with a trusted signature!
 p :          There is no indication that the si nature belon s to
the owner.
Primary key fingerprint: A34A B306 90A3 A042 61F6  163F 2B57 FA04
       A
kun lao opensuse:~>
```

Παρατηρήστε ότι στο προηγούμενο παράδειγμα ο Kung Lao (παραλήπτης) βλέπει ότι έχει μια «καλή υπογραφή» από τον subZraw (αποστολέας), προειδοποιείται όμως ότι δεν υπάρχει καμία διασφάλιση για το αν η υπογραφή όντως ανήκει στον subZraw. Μπερδευτήκατε; Λογικό. Το θέμα εδώ είναι ότι δεν μεσολαβεί κάποια ανεξάρτητη αρχή πιστοποίησης (certification authority, CA), η οποία να βεβαιώνει ότι το φυσικό πρόσωπο "subZraw" πράγματι έχει αυτή τη φυσική υπογραφή. Όμως το θέμα των CA είναι για άλλο άρθρο.

Ας δούμε τι συμβαίνει όταν υπογράφουμε ένα αρχείο χωρίς την παράμετρο --detach-sign:

```
sub  opensuse:~>  p  --si n parabin .odt

 ou need a passphrase to unlock the secret ke  for
user: "subZraw (Underworld SA) <subZraw@defiant.gr>"
    -bit  A ke            A  created     -  -
sub  opensuse:~>
```

Δημιουργείται ένα νέο αρχείο, το parabing.odt.gpg. Αυτό είναι που θα στείλουμε σε άλλους χρήστες. Με την προϋπόθεση ότι διαθέτουν το δημόσιο κλειδί μας, απλά θα τρέξουν το gpg «πάνω» στο αρχείο:

```
kun lao opensuse:~>  p  parabin .odt. p
 p :  i nature made Thu     ar         :  :   A    T usin    A ke
        A
gpg: Good signature from "subZraw (Underworld SA) <subZraw@defiant.
 r>"
 p :                 aka "sub raw  This ain t  im  eam   sub raw
parabin .com>"
gpg: WARNING: This key is not certified with a trusted signature!
 p :          There is no indication that the si nature belon s to
```

```
the owner.
Primary key fingerprint: A34A B306 90A3 A042 61F6  163F 2B57 FA04
        A

kun lao opensuse:~> ls -lh parabin .odt
-rw-r--r--   kun lao users      ar      :   parabin .odt
-rw-r--r--   kun lao users      ar      :   parabin .odt. p
kun lao opensuse:~>
```

Το αποτέλεσμα είναι ότι παίρνουν μια βεβαίωση για «καλή υπογραφή», καθώς και το ίδιο το έγγραφο, στο παράδειγμά μας το parabing.odt.
Όπως είπαμε και πριν, μπορούμε να κρυπτογραφούμε και ταυτόχρονα να υπογράφουμε. Να πώς:

```
sub  opensuse:~>  p  --armor --output parabin  u.odt. p  --recipi
ent " un   ao" --si n --encr pt parabin .odt

 ou need a passphrase to unlock the secret ke  for
user: "subZraw (Underworld SA) <subZraw@defiant.gr>"
    -bit  A ke             A  created     -  -
sub  opensuse:~>
```

Με μια κίνηση μόλις κρυπτογραφήσαμε και υπογράψαμε το αρχείο parabing.odt δημιουργώντας το parabing4u.odt.gpg, το οποίο προορίζεται για τον Kung Lao.
Ιδού τι θα πάρει εκείνος, όταν επιχειρήσει να το αποκρυπτογραφήσει:

```
kun lao opensuse:~>  p  --output parabin .odt --decr pt parabin
  u.odt. p

 ou need a passphrase to unlock the secret ke  for
user: " un   ao   elative of  iu  an    kun lao freemail. r>"
    -bit  A ke       AA       created     -  -    main ke


 p : encr pted with     -bit  A ke       AA       created      -
  -
      " un   ao   elative of  iu  an    kun lao freemail. r>"
 p :  i nature made Thu     ar        :  :   A    T usin    A ke
         A
gpg: Good signature from "subZraw (Underworld SA) <subZraw@defiant.
 r>"
 p :                aka "sub raw  This ain t  im  eam   sub raw
parabin .com>"
gpg: WARNING: This key is not certified with a trusted signature!
```

```
 p :          There is no indication that the si nature belon s to
the owner.
Primary key fingerprint: A34A B306 90A3 A042 61F6  163F 2B57 FA04
        A
kun lao opensuse:~>
```

Αφού πληκτρολογήσει το passphrase του ιδιωτικού του κλειδιού, θα λάβει μια βεβαίωση για «καλή υπογραφή» από τον subZraw, θα πάρει και το ίδιο το parabing. odt. Φυσικά, οποιοσδήποτε άλλος χρήστης θ' αποτύχει:

```
mblack:~ cvar$  p  --output parabin  me.odt --decr pt parabin  u.
odt. p
 p : encr pted with   A ke       AA
 p : decr ption failed:  o secret ke
mblack:~ cvar$
```

GNUPG GRAPHICAL FRONT-ENDS

Όσοι δεν έχουν εύκολη πρόσβαση στη γραμμή εντολών ή απλά δεν θέλουν να τη χρησιμοποιούν καθημερινά, μπορούν να επιλέξουν από μια σειρά graphical front-ends για το GPG. Στη συνέχεια παραθέτουμε εν συντομία μερικά απ' αυτά, για διάφορα λειτουργικά συστήματα και desktop environments.

- **Kleopatra ¦ KDE ¦ Linux**
  Σας αρέσει το περιβάλλον εργασίας του KDE; Αν ναι ξέρετε πολύ καλά τους λόγους, ένας από τους οποίους είναι η πλειάδα προγραμμάτων και εργαλείων που το συνοδεύουν. Το Kleopatra, για παράδειγμα, είν' ένα «Certificate Manager and Unified Crypto GUI», όπως χαρακτηριστικά αναφέρεται στην αντίστοιχη δικτυακή σελίδα. Στην πράξη, πρόκειται για ένα front-end με το οποίο μπορείτε, μεταξύ των άλλων λειτουργιών που προσφέρει, να κρυπτογραφείτε, να υπογράφετε και ν' αποκρυπτογραφείτε αρχεία με το σύστημα του GPG. Εμπεριέχεται στο βασικό πακέτο kdepim4 του KDE, γεγονός που σημαίνει ότι αν δουλεύετε KDE 4.x τότε έχετε ήδη και την Κλεοπάτρα σας. Φυσικά, οι λειτουργίες του Kleopatra είναι διαθέσιμες και μέσα από το Dolphin, το διαχειριστή αρχείων του KDE: Κάντε δεξί κλικ πάνω σ 'ένα αρχείο ή φάκελο, από το αναδυόμενο μενού επιλέξτε το Actions κι εκεί θα βρείτε *και* τις λειτουργίες που προσφέρει το εργαλείο.
- **Seahorse ¦ GNOME ¦ Linux**
  Το Seahorse είν' ένα πρόγραμμα ανάλογο του Kleopatra, όμως για το περιβάλλον του GNOME. Αυτό σημαίνει ότι είναι πολύ πιο απλοϊκό, όχι όμως ανεπαρκές. Λογικά θα βρίσκεται ήδη εγκατεστημένο στο GNOME σας. Σε αντίθετη περίπτωση θα το εγκαταστήσετε με το εργαλείο διαχείρισης πακέτων της διανομής μας. Αν θέλετε το Seahorse να συνεργάζεται με το διαχειριστή αρχείων Nautilus –μεταξύ μας, δεν βλέπουμε το λόγο να *μη* θέλετε–, τότε θα πρέπει να εγκαταστήσετε το αντίστοιχο plugin και κατόπιν να επανεκκινήσετε το

Nautilus. Για παράδειγμα, στο openSUSE θα πληκτρολογήσετε, διαδοχικά:

```
sub  opensuse:~> sudo   pper install seahorse-plu ins-
nautilus
sub  opensuse:~> killall nautilus    nautilus
```

Περιττό να πούμε ότι, αν το Seahorse δεν είναι εγκατεστημένο, η εγκατάσταση του plugin για το Nautilus θα προκαλέσει και την εγκατάσταση του ίδιου του Seahorse.

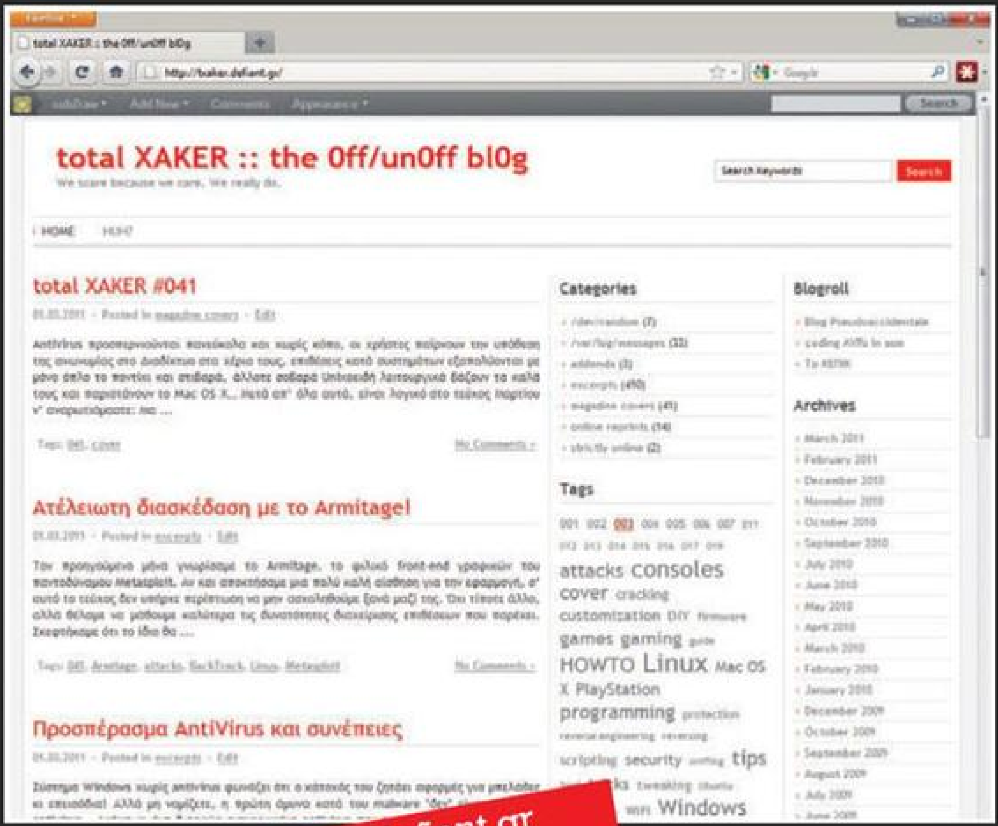
- **KMail ¦ KDE ¦ Linux**
  Το Kmail είναι ο επίσημος mail client για το περιβάλλον του KDE. Υποστηρίζει κρυπτογράφηση/αποκρυπτογράφηση/υπογραφή μηνυμάτων και συνημμένων. Αν *δεν* είστε σαν εμάς και οι 70ριά χιλιάδες επιλογές που προσφέρει το πρόγραμμα *δεν* σας προκαλού σκοτοδίνες, τότε θα το αγαπήσετε. Μάλλον.
- **Evolution ¦ GNOME ¦ Linux**
  Και το GNOME έχει επίσημο mail client και δεν είναι άλλος από το Evolution. Όσον αφορά στην κρυπτογραφία δημοσίου κλειδιού, νομίζουμε ότι είναι περιττό ν' αναφέρουμε ότι υποστηρίζει την αυτόματη κρυπτογράφηση/αποκρυπτογράφηση/υπογραφή μηνυμάτων – γι' αυτό και δεν θα το αναφέρουμε.
- **Gpg4Win ¦ Windows**
  Φυσικά και δεν θα μπορούσε να λείπει από τα Windows ένα GUI για το GPG. Το Gpg4Win (http://gpg4win.org) παρέχει ό,τι θα περίμενε κανείς από ένα τέτοιο ενδιάμεσο χρήσης, όπως, π.χ., υποστήριξη κρυπτογράφησης/αποκρυπτογράφησης μέσα από τον file explorer του λειτουργικού καθώς και σχετικό plugin για το Outlook (Από τους αναγνώστες του περιοδικού, στοιχηματίζουμε ότι το Outlook το χρησιμοποιούν ακριβώς τέσσερις.) Στα εργαλεία που απαρτίζουν το Gpg4Win θα βρείτε και την Κλεοπάτρα ;)
- **GPGTools ¦ Mac OS X**
  Ένας τρόπος για να έχετε το GnuPG στο Mac OS X είναι να το εγκαταστήσετε με τη βοήθεια ενός συστήματος σαν το MacPorts (www.macports.org), το οποίο είχαμε παρουσιάσει εκτενώς στο τεύχος 32. (Παρεμπιπτόντως, το σχετικό άρθρο είναι πλήρως αναδημοσιευμένο στο Επίσημο Ανεπίσημο bl0g του περιοδικού, συγκεκριμένα στη διεύθυνση http://txaker.defiant.gr/?p=3690.) Όμως η εγκατάσταση μέσα από το MacPorts και η μετέπειτα χρήση του GPG προϋποθέτουν ότι είστε εξοικειωμένος με τη γραμμή εντολών κάποιου Unixοειδούς λειτουργικού συστήματος. Τώρα, είναι λογικό να υποθέσουμε ότι από τη στιγμή που διαβάζετε total XAKER δεν μασάτε από την command line. Απ' την άλλη, είναι σίγουρα θετικό το ότι υπάρχει και το πακέτο GPGTools (www.gpgtools.org), το οποίο παρέχει έναν εναλλακτικό τρόπο εγκατάστασης του GPG στο Mac OS X και συν τοις άλλοις έρχεται με μια σειρά εργαλείων για την ευκολότερη χρήση του GPG από το desktop του λειτουργικού. Μεταξύ αυτών είναι το GPGMail, ένα plugin για το Apple Mail που κάνει δυνατές τις λειτουργίες της κρυπτογράφησης, της αποκρυπτογράφησης και της υπογραφής μηνυμάτων μέσα από το ομώνυμο πρόγραμμα.

subZraw

Το Επίσημο Ανεπίσημο bl0g του total XAKER

μ μ μμ , web designer
μ , bl0g total XAKER web!
μ μ μ .
features, μ μ bl0g :

- Επιλεγμένα άρθρα του περιοδικού, πλήρως αναδημοσιευμένα στο web
- Έξτρα άρθρα που δεν έχουν δημοσιευτεί στο περιοδικό, γύρω από τα θέματα που μας ενδιαφέρουν πραγματικά
- Αρχείο όλων των άρθρων που έχουν δημοσιευτεί, για εύκολη αναζήτηση στα αντίστοιχα τεύχη



http://txaker.defiant.gr